Aalto University
School of Business | Mikkeli Campus

CRISIS COMMUNICATION IN ORGANIZATIONAL DATA BREACH SITUATIONS

FACEBOOK DATA BREACH 2018

Seela Suhonen

International Business
Bachelor's Thesis
Supervisor: Mirja-Liisa Charles
Date of approval: 8 April 2019

Aalto University
School of Business
Bachelor´s Program in International Business
Mikkeli Campus

Aalto University
School of Business | Mikkeli Campus

CRISIS COMMUNICATION IN ORGANIZATIONAL DATA BREACH SITUATIONS

FACEBOOK DATA BREACH 2018

Seela Suhonen

International Business
Bachelor's Thesis
Supervisor: Mirja-Liisa Charles
Date of approval: 8 April 2019

Aalto University
School of Business
Bachelor´s Program in International Business
Mikkeli Campus

AALTO UNIVERSITY
SCHOOL OF BUSINESS
Mikkeli Campus

ABSTRACT OF
BACHELOR'S THESIS

Author: Seela Suhonen
Title of thesis: CRISIS COMMUNICATION IN DATA BREACH SITUATIONS: FACEBOOK DATA BREACH 2018

Date: 8 April 2019

Degree: Bachelor of Science in Economics and Business Administration

Supervisor: Mirja-Liisa Charles

Objectives

The main objective of this study was to explore how effective crisis communication can help an organization facing a data breach to minimize the organizational damage caused by the data breach crisis. In an optimal situation, this research explains why certain crisis response guidelines and communication characteristics are useful in data breaches and how they affect the relationship between the organization and the crisis stakeholders. In addition to this, this research should be helpful for all organizations facing a data breach in the future, as it shows from the perspective of a giant global social network company, which forms of crisis communication are useful and which are not.

Summary

This research studies the existing literature on traditional organizational crises and on crisis management and crisis communication and compares the information to modern data breach crises. To use the information from the literature effectively, information from the literature review will be compared to a big data company Facebook's recent data breach in September 2018, affecting initially over 50 million people. The research aim is to find out, how crisis communication is the most effective when an organization is facing a data breach. This bachelor's thesis is a qualitative study and it uses a combination of common effective crisis communication characteristics and a traditional crisis communication theory, SCCT by Timothy Coombs, as guidelines for a recent major data breach case.

Conclusions

The common characteristics of effective crisis communication are still expected from a company facing a data breach by the media and the crisis stakeholders, especially when individuals' personal data is affected. However, a common crisis communication theory SCCT is proven to be mostly incompatible with modern data breach crisis, which means that there is a need for a guiding theory for data breach crisis communication including the characteristics required by the crisis stakeholders and the media. In addition to this, this research concludes that regardless of effective or ineffective crisis communication, the company's prior crisis history and reputation have a significant effect on how crisis communication is responded to.

Keywords: *Organizational crisis, Crisis management, Crisis Communication, Situational Crisis Communication Theory (SCCT), Data Breach*

Language: English

Grade:

TABLE OF CONTENTS

1. Introduction

1.1. Background

Organizational crises have been threatening organizations ever since organizations have been formed. Whether the crisis has been a sudden exit of a key team member, natural disaster (i.e. earthquake), product tampering or fire inside a company, they have always caused organizations damage. Damage can especially happen for organizations reputation which in the end may even affect the organization's overall performance. However, the biggest issue with organizational crises today is their ability to evolve and happen faster than ever. Crises are hectic situations for an organization where actions must be quick and well-thought in order to have the most benefit for an organization facing a crisis. The base for quick and well-thought actions is crisis management, especially crisis communication, which is the most effective way of preventing any further damage and repairing the possible lost reputation of an organization. Crisis communication has always been a key tool for organizations facing crises and in the modern online-orientated world with modern crises, the importance of good and effective crisis communication cannot be emphasized enough.

One important example of modern and evolved crisis is a global issue of data breaches. In today's world, no organization can operate without digital data and all organizations restore the digital data now more than ever. Thus, it is not useless to prepare the possibility of unauthorized access to the organization's secured private data, which might cause organization massive damages in wrong hands. Organizations must be more and more active with developing ways of protecting their privacy, because the ways which attackers can access private information are also developing constantly. Great issue of data breaches, however, lays in the scope which it affects stakeholders outside the organization. When for example personal data of company's customer leak, organizations must take quick actions in order to inform all stakeholders and prevent any further damage, by law and in general. Data breaches continue to be an ongoing problem for all organizations which require a quick and effective share of information in form of well-managed crisis communication which is something all organizations should be familiar with in today's business world.

An important example of a recent major data breach is, for example, Facebook's data breach affecting over 50 million users in autumn 2018. In order to study whether previously researched common and effective crisis communication guidelines and suggestions are still adaptable for modern data breach crisis, this example will be taken into more detail consideration through a case study in this research.

1.2. Research Problem

A lot of research has been already done on effective crisis communication methods in different kinds of organizational crises, but in a quickly evolving and adapting world, new methods for preventing the damage caused by crises are necessary. Especially with the growing need for privacy and security in the digitalizing world, data breaches have become a major threat for many organizations. Cyber attacks develop constantly, and all those who are skilled and wish to enter secured data unauthorized, are developing new ways to access the data. Problem is that many organizations are aware of effective crisis communication methods in common crises, such as fires and contract breaks, but it is not yet confirmed how crisis communication should be done in the most effective way when a data breach of company's secured data happens.

As mentioned, solving the issue of data breaches is urgent for all organizations. It is crucial to have a plan of action in crisis situations in case an organization discovers a data breach. With modern data breach crises, it is possible that the previous effective crisis communication guidelines are still suitable for data breaches, but it is not yet totally confirmed. Data breaches are a relatively new type of crises, which are still widely researched through different cases. Common crisis communication guidelines have been implemented in different cases around the world, but there is still a gap in the field when considering the use of common crisis communication guidelines with data breach situations.

1.3. Research Questions

Research questions for this research are:

1. Do common effective crisis communication methods apply in a modern data breach situation?

2. What, if anything, should be stressed in the guidelines for data breach crisis communication?

1.4. Research Objectives

Based on this research's research questions, objectives of the research are:

1. Find out how common crises differ from modern data breach crises

2. Find out how effective crisis communication can help an organization facing a data breach repair the damage.

3. Assess how different crisis communication methods affect the response of the media or the crisis stakeholders

4. Explain why it is important for organizations to prepare for data breach from the perspective of crisis communication.

1.5. Definitions

Here are the summary definitions for the keywords of this bachelor's thesis:

1.5.1 Data Breach

Data breach means a situation where either identifiable personal information (i.e. names, credit card numbers, social security number, passwords) or other private corporate data, such as strategy plan or other data, leaks to outsiders without a purpose (Baker et al., 2011; Edwards et al., 2016; Perri and Perri,

2018; Romanosky et al., 2014; Rosenbaum and Segarra, 2012; Veltsos, 2012; Wong, 2013). In general, it is a situation where an unauthorized party gets access to protected and private data, which causes organization damage.

1.5.2. Organizational crisis

Organizational crisis is a sudden and unpredictable threat or event for an organization causing stress and pressure that has negative impacts on the organization itself and its stakeholders (Clearfield and Tilcsik, 2018; Coombs and Holladay, 2005; Mishra, 1996; Santana, 2004; Sellnow, Ulmer, et al., 1998; Tierney, 2003; van der Meer and Verhoeven, 2013).

1.5.3. Crisis management

According to Schuetz (1990), the main purpose of crisis management is to provide clear and correct information as quickly as possible for publics outside the organization, which are affected by a certain crisis.

1.5.4. Crisis communication

According to Freberg et al (2013), crisis communication means effective and efficient messages to relevant audiences during an organizational crisis process. In other words, crisis communication includes sending and receiving messages in order to prevent or decrease negative outcomes of an organizational crisis and also to protect the organization, stakeholders and the industry from damage (Coombs, 1999).

These definitions are made to summarize the key concepts of this research. These concepts will be taken into consideration in more detail in the literature review section.

2. Literature review

Introduction

When researching whether the common guidelines for effective crisis communication are adaptable for today's data breach situations in organizations, it is necessary to define a crisis, crisis communication and management and the concept of a data breach. The purpose of this literature review is to provide the base knowledge of organizational crises, how to solve them and how to implicate the resolving methods to data breaches. More specifically, the literature review will study what an organizational crisis is, what are the characteristics of it and what challenges it poses for an organization. In addition, this literature review will investigate what has been done with organizational crisis research and case studies as well as what do crisis management and crisis communication mean and how can they help to solve the crisis. Lastly, research will focus on the main topic of data breaches by defining the concept, listing the characteristics and defining challenges they pose for organizations internationally. The final part of the literature review will compare the traditional organizational crises to more modern data breach crises.

2.1. Organizational crisis

As Milburn, Schuler and Watman state (1983), one of the most significant impacts on the organization and all its members is an organizational crisis. A crisis has an impact on necessary operations of an organization, and in the worst case, even on the organization's lifespan. It also influences the well-being of the organization's members and those whose organization depends on in order to complete organizational processes (i.e. suppliers) (Milburn et al., 1983).

The concern with organizational crises has been increasing due to society's dependence on diverse and large technological and corporate structures (Sellnow, Ulmer, et al., 1998), and it is not going away. Organizational crises keep evolving all the time, and it is no more a question of whether a crisis will strike an organization, only when and how it will strike (Pearson and Mitroff, 1993).

In this section of the literature review, I will define crisis in an organizational context, define different characteristics related to organizational crisis and challenges which a

crisis poses to an organization. The purpose for the reader is to understand what organizational crisis actually means in practice in order to be able to compare it with the modern crisis, data breach, which in the end is the main type of crisis this research will focus on.

2.1.1. Definitions of 'crisis' in an organizational context

Many definitions have been offered for organizational crisis during the years of research. Most researchers agree that organizational crisis is a sudden and unpredictable threat or event for an organization causing stress and pressure that has negative impacts on the organization itself and its stakeholders (Clearfield and Tilcsik, 2018; Coombs and Holladay, 2005; Mishra, 1996; Santana, 2004; Sellnow, Ulmer, et al., 1998; Tierney, 2003; van der Meer and Verhoeven, 2013). It is good to note that stakeholders, in this case, are any group that can affect or be affected by actions taken by the organization (Bryson, 2004).

In addition to crisis definition, according to Coombs (2014, p. 3) the concept 'crisis' can be defined more specifically as ''the perception of an unpredictable event that threatens important expectancies of stakeholders related to health, safety, environmental, and economic issues, and can seriously impact on organization's performance and generate negative outcomes''. In other words, the crisis is an event that creates an issue and keeps it going or gives it more strength (Heath and Palenchar, 2008). However, even if crises are often seen as negative, the word 'impact' is also important. According to Penrose (2000), crises are not necessarily good or bad, but they are often perceived as bad. In addition, the way people see the crisis as an opportunity or threat may also have significant impacts (Penrose, 2000). Crisis can also occur while an organization is growing and provide an opportunity for growth as well as it can give an organization a possibility to achieve its current goals (Milburn et al., 1983).

2.1.2. Characteristics

As mentioned before, crises are unpredictable events that have an impact on the organization. They can cause an organization either losses or gains, and the effect of those comes from how an organization manages the crisis (Milburn et al., 1983). Before defining any specific characteristics of organizational crises, it is useful to give some examples of traditional types of crises. Traditional crises can be easily categorized for example according to Seeger et al (2003) who proposes categorizing

crises into natural disasters (i.e. earthquakes, tsunamis, wildfires), industrial accidents (i.e. explosions, product failures, spills) and intentional events (i.e. product tampering, violence at a workplace, terrorist attacks). These are a few common examples of crises, but not all possible crises there are. To continue the listing, crises can include technology breaks, disruptive moves of a computer, failure of a promising project, promising employee leaving the company, negative reaction to a new product from consumers and so on (Clearfield and Tilcsik, 2018). However, differentiation between different crises is in important for finding the correct solutions for crisis situations (Seeger, 2006).

Differentiation between crises can, for example, be done through categorizing. When crises are categorized based on their characteristics, there are almost as many ways of doing It as there are researchers. However, this research will focus on Coombs (2007) categorization, where crises are categorized into crisis clusters according to three different types: victim, accidental and preventable crisis clusters. Overall, other researches have categorized crises often for example based on their original cause, location, and environment. In Egelhoff and Sen's (1992) research, for example, crises are divided into four categories based on the type of failure and the source of failure: technical and sociopolitical types, and remote and relevant environmental causes.

Continuing on important characteristics of organizational crisis, there are also two possible environments where a crisis may take place: external and internal (Milburn et al., 1983). External environment includes competitors, suppliers, clients and customers, regulators, society, owners, boards of directors and natural disasters. These concepts can be seen as components that play a crucial role in the external environment and organization mismatch. However, if the external environment is under control and predictions of its effects can be made, causes for the organizational crisis are most likely due to Internal environment. The internal environment of the organization includes four classes that are executive characteristics (i.e. personality, knowledge), experience and history, demographics (i.e. age, size, values, products, location) and attributes (i.e. degrees of centralization, buffering, diversity, structural flexibility).

.

To conclude the characteristics of organizational crises, crises are usually rare and unexpected events and they will most likely pose a threat and stress for the organization. In other words, three main characteristics of an organizational crisis are unexpectedness, rareness, and threat. Crises may also cause organization and its

stakeholders' either positive or negative impacts on different scopes from various reasons either from outside or from inside of the organization. The crisis requires an organization to act in order to improve the situation into the direction which the organization wants. In the end, the optimal result is minimized damaged caused by the crisis.

2.1.3. Affects and challenges for organizations

Challenges organizations face after a crisis may be affected due to multiple factors. For example, the importance of organizational goals affected in a crisis and the amount of uncertainty with solving a crisis may affect how serious the crisis is for the organization. Also, the dynamic environment of the crisis, misunderstanding between an organization and environment, positive vs. negative effects from the crisis, amount of members affected, personal perceptions of the crisis and match between stated goals and the organization are important factors to consider when talking about challenges for an organization in a crisis (Milburn et al., 1983). These factors also affect how the organization should handle issues related to crises. According to Coombs (2007), crises may cause both reputational and financial threat for the organization as well as they can harm stakeholders financially, physically or emotionally.

The reputational threat is one of the most important aspects of organizational challenges when looking at a crisis. As mentioned in the previous chapter, reputational threat poses organization a challenge as it may easily affect its stakeholders and its strategic position, and it is crucial to maintaining it as well as possible (Abraham and Tishler, 2005; Claeys et al., 2010; Coombs, 2007; Coombs and Holladay, 1996; Schultz et al., 2011). Reputation tells about the organization's structure and its variety of activities and it is easily affected by customer's satisfaction. It is also associated with the firm's growth and accumulation of customer orders, but not necessarily associated with profitability, the share of the market or financial strength. (Abraham and Tishler, 2005). Reputation is easily affected also through organizational responsibility in a crisis situation (Coombs and Holladay, 1996), which varies according to crisis situations. It is crucial for an organization to have a proper crisis response in order to prevent for example boycotts and to repair the reputation (Schultz et al., 2011). However, research shows that most important factor when repairing the reputation is organization's capability to eliminate preventable crisis possibilities as it is the most harmful type of crisis for organizational reputation (Claeys et al., 2010). Preventing preventable crises is just one of the examples for effective maintenance and repairing of the reputation

according to Coombs (2007), which will be discussed later in this literature review in more detail.

If the organization's reputational challenges are not repaired, they can translate into financial issues that may even threaten the organization's survival (Coombs and Holladay, 1996). For example, McDonald and Härtel (2000) listed cases in their research, such as recall of 620 000 Mitsubishi cars and trucks in Japan, which ended up costing millions of dollars in recall costs and fuel contamination. It is therefore clear, that financial state is important for an organization's survival and operations, and to stakeholders, such as customers. Romansky et al (2014) state that if a customer of an organization suffers financial damage, the organization will more likely face a lawsuit in a crisis situation. Financial state is also crucial constraint when it comes to affording the reparation after the crisis (Coombs, 2007). On the other hand, the organizational crisis may as well be based on financial issues which require also effective methods of crisis management and communication.

To conclude, what organizations give to the public in crisis may both have an impact on their reputation as well as the financial situation. The extent to which an organization's response affects the reputation and financial state can also affect an organization's general image. Meaning that the biggest challenge for organizations in a crisis is to have an effective response plan in order to repair the reputation and financial state of the organization. However, the most important aspect for organizations to notice is stakeholders' physical and psychological needs should be organizations top priority in a crisis before turning the focus into reputation and financial damage (Coombs, 2007). They will most likely expect an organization to react and act in a crisis, and that is what the organization should do in order to maintain the relationship between it and the stakeholders.

2.2. Research approaches to organizational crises

2.2.1. Findings from case studies

Organizational crises have been often researched through case studies, which is the most popular method for these kinds of studies. Results mostly focus on what should have been done in a case and/or what could be done in the future with a similar situation. In addition, most information in this literature review is based on articles

which have conducted case studies. To show few examples from the findings, Clearfield and Tilcsik (2018) for example concluded that company should learn to stop when things are going wrong, do clear monitoring and diagnosing on the ongoing issue and make sure that every member of the organization knows what other parts of the organization are doing. This was based on Nasdaq's case where a system bug ended up blocking orders for 20 minutes and costing millions of dollars for the company. Cole and Fellows (2008) on the other hand focused on communication failure with Hurricane Katrina, where communication ended up having 'inadequate clarity', 'insufficient creditability' and a failure to properly communicate to critical audiences. They concluded that in crises like this, communication should have consensus and adequate crisis messages, be credible to the respondents and demographic characteristics (class, gender, ethnicity) of the audience should be adapted in order to have an effective crisis communication.

Based on case studies, Seeger (2006) also stated about crisis communication messages that self-efficacy, such as simple encouraging of stakeholders to monitor the media for additional crisis developments, might restore a sense of control and help reduce the harm of risk factors in uncertain situations. In addition, older research of Sellnow et al (1998) studied a 1994 salmonella outbreak at Schwan Sales Enterprises and concluded that corrective actions through effective crisis communication and management (in this case i.e. refunds, compensations, and hotlines for customers) can enhance image restoration strategies, such as denial, bolstering and mortification. Ulmer et al (2007) later added that also renewal is important in addition to image restoration for an organization facing a crisis. In addition to this, Acquisti et al (2006) added, from the field of data breaches, that lack of complete information about how companies protect their personal information gives insufficient signals to consumers when it comes to correcting the imbalance by themselves.

2.2.2. SCCT, situational crisis communication theory

The main theory of the research, Situational Crisis Communication theory, has been developed by Coombs (2007) to help organizational crisis managers handle different crisis situations in terms of maximizing the reputational protection in a crisis as an alternative approach for case studies. According to Coombs (2007), theory draws 'speculations' conclusions about the utility of crisis response strategies. He uses the term 'speculations' since according to the research, case studies limit people's

understanding of how to respond to crises and about crisis response strategies. The theory provides a prediction on how organizational stakeholders may react in terms of reputational threat to different types of crises and a theoretical framework to help to understand on how crisis communication can be used as an asset in organizational crises. In other words, SCCT tries to match the crisis response strategies to specific crisis situations in order to restore the organizational reputation in the best way possible (Claeys et al., 2010). Based on the research, the theory will provide a set of ''evidence-based crisis communication guidelines'' for crisis managers and help them to choose the correct responding method of crisis communication based on specific crises. More specifically, SCCT theory identifies how key aspects of a crisis affect crisis causes and the stakeholders' view of an organization's reputation (Coombs, 2007, p. 1).

It is important to notify that SCCT bases on Bernard Weiner's theory (1985) of motivation and emotion, which is called the Attribution theory. Attribution theory provides a base for the relationship between variables used in the SCCT theory and shows that crisis is seen as a negative event which leads stakeholders to estimate the crisis responsibility (Coombs, 2007). In short, attribution is a causal explanation for behavior or an event (Harvey and Martinko, 1982). Attribution theory's primary objective is to study causal ascription relationship, which plays a crucial role when researching emotions and motivations. In other words, theory expects that people try to determine causes for certain outcomes of other people's behavior or events (Weiner, 1972). In practice, causal ascription relationships are being researched by looking first at the outcome of a situation and after that trying to find a cause for it (Weiner, 2006). The SCCT theory is helpful for example to managers who may assist employees by providing honest perceptions of the causes for their performance and for employees themselves (Harvey and Martinko, 1982).

2.2.3. Crisis clusters of SCCT

When managers use SCCT, they must understand the crisis situation and decide which response strategy is the most suitable one for a certain crisis in order to protect their reputation (Coombs, 2007). In order to choose the right strategy according to the theory, managers must be able to estimate the level of reputational threat for the organization in a crisis. In this case, reputational threat means the damage amount a crisis can cause for organization's reputation if no actions are taken, and it is shaped by three factors: *initial crisis responsibility, crisis history, and prior relational reputation*.

To explain the three factors, initial crisis responsibility means how much the stakeholders see the organization as responsible (Coombs, 1995), crisis history looks whether an organization has had a similar crisis before and prior relational reputation sees how well or badly the organization has treated its stakeholders in general previously.

The SCCT theory suggests that managers follow the two-step process when using the three factors, which are 1. Determining the initial crisis responsibility attached to crisis and 2. Assess the crisis history and the prior relationship. First, according to the SCCT theory, each type of crisis has ‘’specific and predictable levels of crisis responsibility-attributions of organizational responsibility for a crisis’’(Coombs, 2007, p. 6). In order to do this, Coombs (2007) created three crisis clusters, *victim cluster, accidental cluster* and *preventable cluster (*or *intentional cluster)*, which each include a similar level of crisis responsibility for the organizational crisis. In other words, the first step for a manager means placing crisis into a cluster in order to predict the crisis responsibility for stakeholders (Coombs, 2007).

Victim cluster describes crises where someone or something else caused the crisis other than the organization. This causes the organization to be seen as a victim (i.e. natural disasters). In accidental crises, the crisis is caused by unintentional actions of an organization (i.e. technical error accident). With the preventable crisis, an organization is purposely taking actions that may lead to a crisis (i.e. human-error accident) (Coombs, 2007). Crisis types and clusters are introduced more specifically presented in Appendix 1. According to the second-step introduced for managers when evaluating the reputational threat, managers need to assess organization’s crisis history and prior relationship reputation factors, which are the two initial and intensifying factors for the assessing (Coombs, 2007).

2.2.4. Crisis response strategies of SCCT

According to Coombs (2007), crisis response strategies can decrease the negative impact of a crisis and help to repair organizational reputation as well as shape organizations position in a crisis. SCCT aims to create a list which has a conceptual connection with the crisis clusters, and in this case, the link is the responsibility. The theory provides three primary crisis response strategies, *deny strategy, diminish strategy and rebuild strategy*, and one secondary response strategy, *bolstering strategy*. The strategies are represented in more detail in table 2 (Appendix 2) and

explained in the next paragraph. SCCT theory includes also guidelines for the usage of the response strategies, which are represented in table 3 (Appendix 3) and discussed further in the methodology section. However, it is good to notify that it is nearly impossible to create a perfect list for crisis response strategies. Instead, a list of useful crisis responses can be created (Coombs, 2007).

Deny strategy tries to remove all connections between the organization and the crisis. The aim is to not suffer any damage from the crisis by not being involved in it. It requires managers to argue that there is no 'real' crisis and they need to deny the truth to rumors and mute the acquisitions for immoral conduct. Deny strategy is successful when stakeholders and media believe that the organization is not involved or responsible for the crisis, and reputational harm does not happen (Coombs, 2007).

Diminish strategy's aim is to make crisis seem less bad to the public or show that the organization had little control over the situation. If the strategy is successful, crisis managers can make people think about the crisis less negatively and reduce the damage to the organization. This strategy, however, needs evidence to support the arguments which still doesn't ensure its success. If the public sees the crisis and the organizational responsibility differently, the damage is still happening for the organization. The diminish strategy is the most effective when it is reinforcing existing frames of a crisis (Coombs, 2007).

Rebuild strategies may create new reputational assets for an organization. Managers may present positive and new information about the organization and remind stakeholders of past positive experiences (work etc.). These strategies try to improve the reputation of an organization by providing ''material and/or symbolic forms of aid to victims'' (Coombs, 2007, p.10). In other words, the point of the rebuild strategy is to put negatives to side by bringing up the previous positive aspects. Managers will try and replace the damage of a crisis by taking positive actions when a crisis presents a severe reputational threat (i.e. accidental crises or intentional crises with crisis history and bad prior relationship reputation). Rebuild strategy might, however, be the most expensive one to use (Coombs, 2007).

Bolstering strategies provide a small opportunity to develop reputational assets. With these strategies, stakeholders may try to appeal to stakeholders' goodwill if they have had positive relationships with them previously in order to protect the organizational reputation. This means for example managers praising stakeholders' efforts during a

crisis and tries to draw sympathy for the organization. Bolstering strategy may also remind about good past works in order to balance the negative outcomes from a crisis. The strategy is best used as a supplement to the other three primary strategies and adjusting information (Coombs, 2007).

Even though SCCT is one of the most known crises communication theory, it has also been criticized. For example, Clayes et al (2010, p. 6) studied SCCT and concluded that ‘’matching crisis types and crisis responses do not lead to the more positive perception of firm reputation than mismatches’’. They also did not find any significant difference between the victim crisis and the accidental crisis in reputational perceptions. Clayes et al (2010) also mention that rebuild strategies have more positive impacts than diminish strategies. It is also good to notice that personal locus of control, which according to Clayes et al (2010, p. 6) as a trait of personality has ‘’a moderating impact on the effect of response strategy on reputation’’ is not included in the SCCT theory. For example, people with an external locus of control prefer to *deny response strategy* more than people with internal locus of control (Claeys et al., 2010). However, regardless of the critique, SCCT is still one of the most widely used theory in the field of crisis communication research and it has stayed as a base theory for crisis communication since its developing.

2.3. Crisis management

The basic idea of crisis management is that its primary objective is to provide clear and correct information as quickly as possible for publics outside the organization affected by the crisis (Schuetz J., 1990). As mentioned in the previous sentence, the key idea of why crisis management is discussed in this review is that it also includes providing ‘clear information’ when a crisis occurs. In other words, efficient management needs also efficient communication in order to succeed. However, one specific definition for crisis is also that management is a continuous, integrated and comprehensive effort that organizations effectively put into place in order to understand and prevent a crisis. When crises occur, they are effectively managed considering each step of their planning and training activities and the interest of their stakeholders (Santana, 1999). It also requires the organization to develop management strategies in order to deal with the crisis (Milburn et al., 1983).

Most important issues related to crisis management can be for example crisis anatomy, risk perception, crisis incubation and destination image (Santana, 2004). Crisis management is not just a strategic and reactive response to a crisis, but rather a prepared discipline including inter-related processes from crisis prevention and preparedness to crisis response and crisis recovery (Jaques, 2007). In practice, crisis management may, for example, include structure design, crisis team selection, team training, crisis situation audit, contingency plan and the managing of the crisis (Littlejohn's Six Step Model, 1983). To conclude, crisis management is a process that requires the organization to plan and act in order to prevent as much as possible of the organizational damage. This includes especially the important aspect of crisis communication, which is discussed in the next chapter.

2.4. Crisis communication

Overall, crisis communication is the most effective way to affect stakeholders and that way ultimately amount of organizational damage. It is good to also note that this research studies the concept of crisis communication, not the concept of risk communication. Risk communication is usually about anticipating disasters and sending messages as a warning, cautionary, prevention or avoidance, and crisis communication usually about the decrease of disruptions and social harm during and after the crisis in addition to the handling of public relations (Andersen and Spitzberg, 2009; Reynolds and Seeger, 2005).

2.4.1. Definition

Crisis communication can be seen as a tool for long-term benefits for an organization in a crisis (Sturges, 1994). According to Freberg et al (2013), it means effective and efficient messages to relevant audiences during an organizational crisis process. In more detail crisis communication ''seeks to explain the specific event, identify likely consequences and outcomes, and provide specific harm-reducing information to affected communities in an honest, candid, prompt, accurate, and complete manner'' (Reynolds and Seeger, 2005, p. 4). In addition, Coombs (1999) earlier stated that crisis communication includes sending and receiving messages in order to prevent or decrease negative outcomes of an organizational crisis and also to protect the organization, stakeholders and the industry from damage.

A most important characteristic of crisis communication is informative communication about the crisis event for the crisis stakeholders. In addition, crisis communication is infrequent and spontaneous communication which includes, for example, the cause of the crisis and current state of the organization, press conferences and/or releases, speeches and websites, communication through different media (i.e. news), and general messages for the public (Reynolds and Seeger, 2005). Overall, many crisis communication definitions suggest that crisis communication should be transparent and efficient communication to relevant audiences when an organization is facing a crisis in order to save the organization from damage (i.e. reputational and financial). Messages may also be personalized and provide the next steps of action to some extent in order to be efficient (Freberg et al., 2013) but in practice, it may be challenging. In general, communicating during a crisis may be difficult because an instant response is necessary, the situation is uncertain and the organization is facing a threat (Ulmer et al., 2007) but it doesn't remove the fact that it is necessary for an organization that wants to minimize the damage of a crisis.

2.4.2. Purpose of Crisis Communication

According to Andersen and Spitzberg (2009) communication in a crisis is the most important tool in gaining cooperation from the public and linking responders. Sturges adds (1994) that crisis communication policies and strategies may lead to positive opinion development of important stakeholders for an organization Coombs (2007) further suggests in his SCCT research that crisis communication is crucial for protecting organizational reputation. However, the most important thing in a crisis is to protect all stakeholders from any harm through crisis communication. In practice, this means providing stakeholders with the information they need in order to protect themselves (Coombs, 2007). Coombs (2007) states that it is the ethical responsibility of an organization. After stakeholders are informed, Coombs (2007) suggests that actions the organization is doing in order to protect crisis stakeholders are informed as well as start the reputation repairing. Even if the reputation is a great threat for an organization, it is the most ethical approach to consider the organization's stakeholders first.

An older study of crisis communication makes a suggestion that it is important to move into corrective actions that still are a severe part of the image restoration process of an organizational crisis (Sellnow, Ulmer, et al., 1998). When moving into the protection of

the reputation, multiple things count. As mentioned, crisis communication is effective communication to a relevant audience in order to reduce negative outcomes for an organization in a crisis. During the years of research, there have been multiple arguments on what are the best practices of crisis communication. Based on an expert panel, Seeger (2006) suggests a list of ten best practices of crisis communication which includes honesty and openness, acceptance of uncertainty and ambiguity, communicating with compassion, concern and empathy, meeting the needs of the media and remaining accessible, listening and understanding the public, partnerships with the public, pre-event planning, messages of self-efficacy and process approaches and policy development. These practices base on many researchers' sayings but are just a general and summarized opinion on what should be done in crisis communication. For example, Seeger's study (2006) does not take social media into account, which is a relevant aspect of crisis communication in today's world.

Many researchers do also suggest that planning and creation of certain mechanisms to support the process, spreading and success of crisis communication to pre-identified stakeholders is positive for organizations (Austin et al., 2012; Baker et al., 2011; Coombs, 2007; Seeger, 2006). However, as the older study of Sturges (1994) mentions, crisis communication happens during and after the crisis and the communication content to the public should be customized based on the ultimate goal of positive residual opinion among the public. Information should also be quickly shared in order to minimize the possible psychological threat of stress, caused by uncertainty (Sturges, 1994). Points in Sturges (1994) research are however made when social media was not a relevant part of crisis communication. They do provide a base for guidelines of crisis communication but in general, fast spread of crisis messages is more of a norm than the exception with today's media channels, which makes the decrease of stress and uncertainty of stakeholders in a crisis easier.

About the message itself and the spread of information to the public in order to protect the reputation, research suggests that the medium is more important than the message (Schultz et al., 2011; Utz et al., 2013). Schultz et al (2011) suggest that even if people talk more about newspapers, tweets have a more positive effect on secondary crisis communication and reactions. In addition, an organization that uses social media to inform stakeholders of a crisis shows that it is willing to inform quickly and directly and engage in the conversation (Utz et al., 2013). Utz et al (2013) also concluded in their research that the type of crisis does not affect the reputational damage, but as said, the medium of messages does. This is in contrast to Benoit (1997) research, which

suggests an organization to focus on the message in order to protect the organizational image. However, it is good to note that the research is significantly older compared to Schultz et al (2011). In addition to 'new' mediums of communication (i.e. social media), it is also crucial for an organization also to remember traditional ways of crisis communication (i.e. journalists, newspapers), since they are still holding the 'credible' image when it comes to shared information (Utz et al., 2013). According to van der Meer et al (2013), the news media has a soothing effect on panic and speculation of the public, meaning it has the potential to prevent crises from escalation.

Even if the research shows that medium matters more than the message itself, the content of messages should still not be overlooked. According to Yang et al (2010) research conducted on individual's interpretations on crisis communication messages, openness to dialogic communication is crucial in creating and enhancing audience's engagement in crisis communication. In fact, sometimes in severe crisis situations, organizations might reduce the public panic by not giving all the available information to the public while it actually provides a better outcome to take the open and dialogical approach (Tierney, 2003). In addition, crisis narratives can be an effective tool in crisis communications when tackling the most difficult challenges, negative emotions of the participants (i.e. frustration, anger, disappointment), significantly after reading the narratives. (Coombs and Holladay, 2005; Tierney, 2003; Yang et al., 2010).

Crisis communication should also be efficiently structured in order to provide the best result in protecting and repairing the organizational reputation. This means mostly the consistency, which should exist between all organizational crisis communication per a certain crisis. In general, the efficient structure of crisis communication messages also means the way a certain message is presented (i.e. chosen words, sentences, images). One example of crisis message structuring can be for example one of the crisis types because they all feature certain aspects of a certain crisis (Coombs, 2007). Forming of the messages correctly guides also readers thoughts (Coombs, 2007) and the way message how problems, causes, attributions of responsibility and solutions are defined and seen by people (Cooper, 2002).

Most importantly, structuring of the crisis messages means things the author wants to emphasize in a message for the respondents. Readers of the message will, therefore, focus their attention to certain things in a message (Druckman, 2001). For a crisis manager, this is an important aspect because the certain structure of the message affects stakeholders and their opinions about an organization. For example, the

mentioned structuring of the message according to the crisis type affects how much stakeholders consider the organization to have crisis responsibility in a crisis (Coombs, 2007). However, it is also good to note that in general personality of the decision-maker (writer) also affects the crisis communications and therefore also the perceptions on organizational crises and crisis communication methods used in them (Milburn et al., 1983).

2.5. Data breach: A modern day organizational crisis

Data breaches in organizations are a continuous concern for all organizations that contain private information. In addition, the concern with data breaches are increasing with the number of cases published and the legislation on data breaches will most likely increase at the same time. Data breaches have existed ever since organizations started keeping records and store personal data, even if often they are linked to digitalization (Perri and Perri, 2018). Most importantly data leaks pose an ongoing and evolving threat to financial and personal security as well as they bring costs for organizations that held a large amount of personal data (Edwards et al., 2016). In other words, a data breach is a crisis organization might face and needs to prepare for in order to minimize the damage.

2.5.1. Definition

A data breach can be defined in multiple ways based on what has happened. However, in general data breach means a situation where either identifiable personal information (i.e. names, credit card numbers, social security number, passwords) or other private corporate data, such as strategy plan or other data, leaks to outsiders without a purpose (Baker et al., 2011; Edwards et al., 2016; Perri and Perri, 2018; Romanosky et al., 2014; Rosenbaum and Segarra, 2012; Veltsos, 2012; Wong, 2013). In other words, a data breach is a confirmed incident where sensitive, confidential or other protected data has been accessed or revealed by an unauthorized participant (Rouse, 2017). In addition to personal data losses, the company may suffer from a loss of critical data, business interruption, burdensome disclosure requirements, regulatory scrutiny, third-party litigation, and loss of reputation (Breaux et al., 2014). As well as traditional crises, such as fire or losing an important employee, data breaches cause pressure and stress for the organization and require actions in order to stay on the positive side. There is always also a risk that an organization may receive some

penalties or fines in addition to other costs that come from preventing future breaches (Perri and Perri, 2018).

2.5.2. Characteristics

Often data breach first reminds of a massive hacking attack into organization's sensitive data but for example, even unauthorized hospital employee seeing protected patient data is considered as a data breach (Perri and Perri, 2018; Rouse, 2017). Overall, according to Verizon's 2018 Data Breach report 73% out of 53 308 security incidents (2 216 data breaches included) cases studied were done by outsiders and the rest by insiders. Naturally, part of the cases were also accidents caused by errors, such as employee sending an email to a wrong person. Causes for breaches can also be hacking, malware, misuse, physical causes, social causes, partners, availability, confidentiality, integrity as well as the unknown causes (Verizon Communications, 2018). Sometimes breaches might be also hard to discover and when they are discovered, an organization must immediately take necessary actions in order to protect the organization from all possible aspects (Breaux et al., 2014). In general,

2.5.3. Challenges for organizations

Biggest challenges for organizations in all kinds of data breach situations are its privacy (private data etc.) and the possible reputational damage. On top of privacy losses and reputational damage, an organization will most likely also suffer financial damages in a data breach crisis. In addition to early mentioned penalties and fines, the organization may also face lawsuits if a stakeholder is harmed in any way. In addition to financial damage and chance of lawsuits mentioned in the organizational crisis chapter, according to Romansky et al (2014), an organization has in fact 3,5 times higher chance of being sued by stakeholder if they have suffered any financial damage. Challenge also comes from the fact that when a data breach occurs, actions must be taken fast in order to maximize organization's legal rights and obligations and minimize extra costs and potential liability to claims by regulators and plaintiffs (expending deadlines) (Breaux et al., 2014).

Overall, organizations often try to prevent attacks coming from outside the organization but especially the threat posed by insiders is hard to control because general signs might be hard to spot if someone is using their authority wrong. In addition, discovering any data breach may take time for an organization, and often the discoverer is a third party (i.e. partner). In the worst case, a customer of the organization discovers the

breach which may cause severe reputational damage for the organization (Verizon Communications, 2018). As a conclusion, shareholders are strictly following these kinds of crises which is why it is important that they are handled right. As Coombs (2007) mentioned, stakeholders' well-being is the priority for organizations.

Another important challenge for organizations is also the fact that data breaches are evolving all the time. Cybercriminals are getting smarter and evolving new ways to enter the company's data which means protectors of data must evolve with them and keep up with all updates of the security world (Hayden, 2013). Many different parties have been creating guidelines and regulations in order to control sensitive data and to prevent data breaches. For example, Romansky et al (2011) mention that protection, generating policy debates and significant lobbying is becoming more and more the main focus of regulations. However, if personal data is misused, organizations are most importantly suggested (usually also obligated) to note individuals and take legal actions (Hayden, 2013; Rouse, 2017). For example, in the U.S., many states require organizations to notify all individuals affected by a data breach when personal data has leaked (Fisher, 2013; Romanosky et al., 2011). EU has also regulations for data breaches, such as the provider's need to report to national authority responsible for data protection or to the communications regulator without any delays (Wong, 2013). At lower levels, specific organizations may also have their own regulations to provide a framework for required safeguards, storage, and use practices for handling sensitive information (i.e. hospitals) (Perri and Perri, 2018). However, this does not prevent those incidents from happening.

Preventing of the breaches mostly follows commonsense security guidelines. According to Rouse (2017), an organization should have well-known security basis including vulnerability and penetration testing, proven malware protection, strong passwords, and necessary software patches applied. In addition, security policies should be well-written and handed to all employees, security awareness should be trained continuously, and education should be provided. Breaux et al (2014) and Verizon Data Breach report (2018) also state some guidelines for companies facing a data breach. Breaux et al (2014) suggests that when a data breach is discovered, an organization should as soon as possible assemble the crisis team, contact legal counsel, be cautious with terminology, consider hiring a forensic investigator, review insurance contracts, consider contacting law enforcement, analyze disclosure obligations, consider the prospect of litigation and manage all public relations.

Verizon's report continues that organizations should be alert about possible breaches already before someone else (i.e. legal system) notices them and keep the private data available only to those who need it. In addition to this, the organization should always have their anti-virus systems updated, have two-way authentication to sensitive data and not to forget also the physical security (i.e. security cameras), since all breaches don't happen online (Verizon Communications, 2018).

2.6. 'Traditional' and 'Modern' crises compared

It is easy to state that traditional crises, such as fires or workplace violence in an organization differ a lot from modern cases. By modern cases in this section, the focus is on data breaches which are getting more and more attention each year. Despite the differences, both crisis types also share multiple similar characteristics. Based on the literature review, both types of crises do cause similar stress and pressure for the organization as well as harm to both the organization's reputation and financial state. Crisis management is required for traditional crises as well as for data breach in order to minimize the damage a crisis can cause for an organization. Both crises also do have stakeholders to protect and the optimal goal is to minimize the damage caused by the crisis.

In general, the biggest difference between traditional crises and data breaches are all its victims. In traditional crises, such as harmed products, individuals may return the product. However, when their personal data leaks, their privacy might be in danger. Differences between traditional crises and data breaches lay also for example in the ways which organizations will stop and prevent the crisis. When it comes to crisis communication, for example, both traditional and data breach crises follow mostly the general guidelines, but with data breaches, the direct approach seems to be the most effective. This is because a data breach notification should inform all stakeholders as required by the law and lose the optimism bias and rational ignorance. This will encourage all parties to act and convince them about the problem (Veltsos, 2012). It is crucial for crisis managers to notice this because, in maximum uncertain situations such as data breaches, it is important that all parties are actively following what is happening and are informed directly with all available information.

To continue about preventing a data breach, Verizon's 2018 Data Breach report suggested that in order to prevent data breaches an organization should have all their

digital systems (i.e. anti-virus systems, software) updated all times, which is not necessarily required by most traditional crises (i.e. earthquakes, explosions, product tampering). In addition to this, data breaches will most likely require more procedures with the law than traditional crises (i.e. lawsuit). One great difference is also the fact that traditional crises have been researched more which allows them to have more pre-crisis management methods. Data breaches however still lack clear pre-crisis plans. As Perri & Perri (2018, p. 10) state: ''In the absence of premier practices in the area of crisis management, companies, customers, and jobs are lost''.

It is important for the reader to understand the concept of data breach and how it differs from traditional crises. Both crisis types have typical causes, typical ways to prevent crises and typical major issues related to the crisis, which differ from each other. To summarize chapter on traditional crises versus modern crises of data breaches, Figure 1 presents the key points of both crisis types:

Traditional Crises	Data Breaches
Crisis causes (examples): • Natural disasters • Operation failures (i.e. product tampering) • Employee issues (i.e. key employee leaves the company, contract breaks) • Workplace violence	Crisis causes (examples): • Hacker attacks • Betrayals (i.e. Company's own employee stoles data) • Confidentiality agreement failure (Employee shares the company's private data) • Burglary
Preventing crisis (examples): • Lasting and practical structure of buildings • Good employee satisfaction • Security cameras • Contracts • Organizational rules	Preventing crisis (examples): • Security software • Antivirus systems • Confidentiality agreements • Security Cameras
Biggest issues (examples): • Physical damage to the organization • Unsatisfied consumers (decreased demand) • Unsatisfied employees (possible strikes) • Financial and reputational damage (reputational threat lower)	Biggest issues (examples): • The threat for stakeholders' private data (individuals, other companies) • The threat of the company's own private data (and the possible damage if breached) • Law requirements (i.e. GDPR) • Quick evolvement of crises • Reputational and financial damage

Table 1 Modern Data Breaches vs. Traditional Crises

Overall, modern-day crises still lack the amount of research traditional crises have had. Case studies have been made but there is not yet clear structure between all modern-day crisis studies. It is, however, good to note that traditional crises do serve a good base for modern crisis research. Even if modern crises might be more recent, traditional crises are not going away from organizations. As this research does combine traditional organizational crisis theory SCCT and modern crisis case study, modern crises may use the same approach in the future.

2.7. Conceptual framework

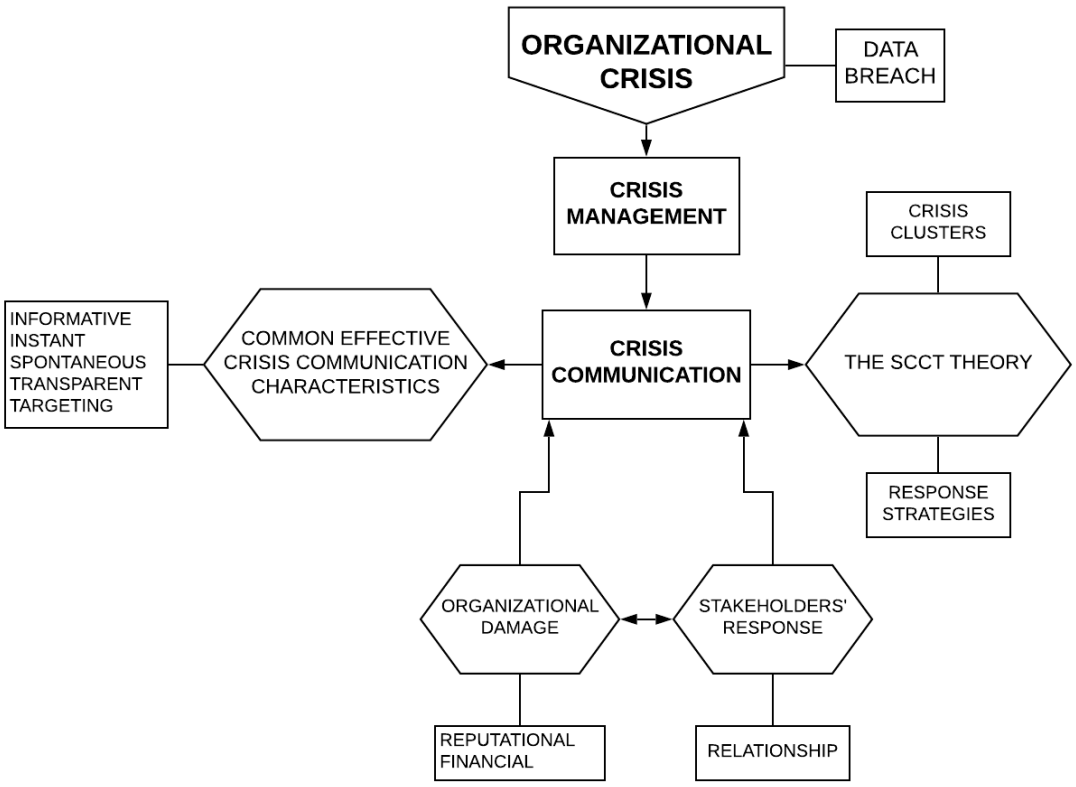

Figure 1 Conceptual framework

In this conceptual framework, the crisis type data breach is included in the main concept, organizational crisis. To solve a crisis, an organization must manage the crisis through crisis management, which includes a crucial part of affecting the amount of organizational damage: crisis communication. Crisis communication itself includes the theoretical approach of Situational Crisis Communication theory by Timothy Coombs (2007) which will be used as a base crisis communication guideline for this research.

The SCCT theory includes crisis clusters and crisis response strategies, which can be matched in a way that the organization gets the maximum amount of benefit from their crisis communication. In addition, common effective crisis communication characteristics should be included in the crisis communication, which is, based on the literature review, informative, instant, spontaneous, transparent and targeting.

With the use of crisis communication, the organization is able to affect both the scope of reputational and/or financial organizational damage caused by the crisis and the stakeholders' response to the crisis, which eventually affects the relationship between the organization and its stakeholders. A relationship exists also between the organizational damage and the stakeholders' response, since the organizational damage may affect stakeholders' relationship between the organization either positively or negatively and vice versa.

Summary

This literature review showed that it is better for an organization to expect the crisis to happen instead of keeping it as an exceptional event. Both traditional and modern crises cause an organization pressure from stakeholders and most likely cause damage to organizations' reputation and financial situation. Thus, it is crucial for an organization to protect stakeholders and inform the stakeholders of the crisis as well as the media, in order to restore the positive image and the relationships. Therefore, an organization should prepare for today's modern and quickly developing crises, so that the organization is capable of minimizing the damage as well as it is capable of minimizing the damage of traditional crises.

Luckily, data breaches have been recently highlighted in the world of organizational crises. More research on data breaches is continuously published and all research aims to prepare organizations for possible data security crises in the future. This is the reason, why this research will focus on the most effective ways of crisis communication and the fact of how the traditional guidelines match with more modern and unknown crisis types. It is clear that the threat posed by data breaches is serious as they are capable of affecting both individuals' and organizations' sensitive and private information. It is highly important for crisis communication to be successful in these crises, as the failure might cause both for the organization and for the stakeholders serious and long-lasting issues.

3. Data and methodology

3.1 Qualitative research: Case study method

This research will conduct a qualitative study that collects data from a data breach case. A qualitative method was chosen for the research because it tries to answer the question ‘’how’’ and ‘’why’’ rather than ‘’how many’’ (Pratt, 2009). Research tries to fully understand the crisis case situation and find the key turning points for future crisis communication research and cases. The goal of the research is to find out key issues of crisis communication occurred in a specific case and the causes and the effects of possible successful and negative moments of crisis communication.

The case method was chosen because it aims to understand the dynamics present within a single setting (Eisenhardt, 1989). It allows the research to explore and understand a complex issue when a holistic and in-depth analysis is required by the study. The case study also lets the research go beyond the statistical analysis of quantitative research and understand the behavioral conditions from the case’s perspective in addition to examining data in a specific context (Zainal, 2007). Typically case study may include multiple different data collection methods (Eisenhardt, 1989), but in this research observations on existing data will be used.

3.2 Data

This research uses data from multiple different online sources published about Facebook’s September 2018 data breach. Data set includes altogether **27** data sources, that include Facebook’s blog posts, the Facebook post of the CEO Mark Zuckerberg, YouTube videos, web articles and Facebook’s Twitter posts in addition to information about Facebook’s possible user amount and stock price changes. Blog posts are from Facebook’s own blog *Facebook Newsroom,* and the posts are made by Facebook VP of Product management Guy Rosen and VP of engineering at Security and Privacy Pedro Canahuati. The Facebook post included in data is made by Facebook’s CEO Mark Zuckerberg. Twitter posts by Facebook are re-sharing the blog posts from Facebook Newsroom and the comments include some reactions from individual users who were affected by the crisis. In addition to these, reactions by the

media are included in the data in the form of web articles and videos made online after the breach was published and informed by Facebook.

Full data of this research is included in this research as Appendix 3. Data is ordered based on the date the data was published, and Facebook's own crisis communication is highlighted with thicker borders and bolded text. The table has been arranged in a way that if the content of the data source presented Facebook mostly in a positive manner or in a neutral, it is marked as an X in the positive ''Pos.'' section and vice versa to negative ''Neg.'' section if Facebook was presented in a negative manner. Facebook's own crisis messages were not categorized (Twitter posts, Facebook post, Blog posts, CNBC video with only FB CEO comments), as it can be assumed that the company tries to present itself as well as possible. Categorization to positive and negative bases on sentence and word choices and the argumentative comments included in the sources. For example, if the data was only informing readers about the case and showing at least some trust or hope for the company, it was marked as a positive. If the data source instead listed negative aspects of Facebook or included public negative comments or negative describing of Facebook, the data source was marked as negative. Differentiation is made in order to analyze how well Facebook's messages about the crisis were taken in different media. In other words, it helps this research to allocate whether Facebook's own crisis communication choices had an effect on the media and its response. In the end, Facebook's possibly changed stock prices and user amounts after the crisis will be taken into focus. These findings will be separately explained and analyzed in the Findings and analysis section.

Data has been collected online during 10.02.2019 – 27.3.2019 and it is fully represented in the data table, Appendix 3. Data is limited to the first two weeks (28.09.2018 – 12.10.2018) after the crisis went public with a few additional information on Facebook's user amount and stock price changes. The time period was chosen in order for this research to be able to look deeply into the immediate reactions of Facebook and the public after it. Later data was included to learn more about what the crisis actually caused Facebook and whether Facebook's crisis communication had anything to do with the final result. The table below shows the summary and the structure of the data used in this research:

Online data source	Amount of data
Facebook Newsroom blog post (B)	3
Facebook posts (F)	1
Website article (A)	16
YouTube -video (V)	3
Twitter posts (T)	4

Table 2 Summary of the data

As mentioned before, Facebook's own crisis communication is highlighted in the data with thicker borders and bolded text. One exception is a CNBC video interview with Mark Zuckerberg, which is counted as Facebook's own crisis communication because the video does not include any other messages. In addition to this, the data has been coded in a way that Facebook's blog posts at Facebook Newsroom are marked as B, Facebook posts as F, Website articles as A, YouTube -videos as V and Twitter posts as T. These codes will be used in the Findings and analysis section and each data source can be found in the data table (Appendix 3). In the data section, each data source is also marked with a number (i.e. Website article 1 = A1) in order to clearly separate different data sources from each other in the findings and analysis section.

3.3. Introduction to Facebook's 2018 September major data breach - case

Facebook's September 2018 major data breach case was chosen for this research as it is from a company that is well-known globally. In other words, Facebook is one of the most recognized companies and brands which makes it a relevant example of today's modern and major data breaches, where a specific use of crisis communication was necessary. In addition, the data breach Facebook had was one of the biggest of the 21st century affecting millions of people and their personal data. It is useful to research a case as large as this in order to find the guidelines for effective crisis communication from an international perspective. In this case, the challenge Facebook is facing from the crisis communication point of view is, for example, convincing the users that the company handles their data privacy (Isaac and Frenkel, 2018).

To explain the case, Facebook's September 2018 major data breach initially affected over 50 million users worldwide by exposing their private personal information. Accounts of users were compromised by attackers, who got access to individual's accounts and all secured personal information contained in them. In more detail, attackers succeeded to exploit a feature in Facebook's code to gain access to private user accounts and possibly take control over them (Isaac and Frenkel, 2018). In other words, hackers were able to use Facebook's ''view as'' feature in user profiles, which allows a user to see their own profile as someone else. Therefore, hackers got access to tokens, which allow users to stay logged into the service without entering the password. These 'digital keys' could then be used to control also other people's accounts (Castillo, 2018). In addition to Facebook user accounts, all other sites that use Facebook's access tokens were threatened (i.e. Instagram and Spotify) (Perez and Whittaker, 2018), but eventually there was no evidence of such hacker activity.

The seriousness of the breach arises from its number of users affected and from the stolen private personal data of individual users. Initially, Facebook announced that the breach affected over 50 million users and additional 40 million users who had used the ''view as'' feature in the past year were logged out from their accounts as safety action. Eventually, Facebook announced that approximately only 30 million people were affected, which included 1 million people whose data was not stolen, 14 million people whose name and contact was accessed and 15 million people who also got their other personal information (i.e. birthday, workplace) in addition to name and contact details stolen. The breach was discovered on Tuesday 25th of September 2018 by Facebook's own engineers and it was fixed on Thursday 27th of September 2018. It is said that the breach is the largest data breach in Facebook's at that point 14-year-old history. (Perez and Whittaker, 2018; Rosen and Canahuati, 2018; Wong, 2018).

3.4. Effective crisis communication

In order to analyze Facebook's crisis communication in their September 2018 case, it is useful to list the most important aspects of effective crisis communication. Based on the literature review, the most important part of effective crisis communication is its informativeness. Crisis communication must include all necessary information considering the crisis in order for stakeholders to understand the situation and its relevance for them. Other key factors of effective crisis communication are also transparency, speed and targeting the crisis messages to the relevant audience of a certain crisis. This means, that company facing a crisis must not hide any important

information from the stakeholders and the messages should be targeted to the stakeholders of the crisis. In addition, crisis communication must be instant, fast and spontaneous after a crisis has occurred and noticed by the organization.

The table below will summarize the key characteristics of effective crisis communication based on the literature review:

Key characteristics of effective crisis communication (based on literature review)
• Informative • Transparent • Spontaneous • Targeting • Instant

Table 3 Main characteristics of effective crisis communication

3.4.1. Situational Crisis Communication theory and the Facebook case

In addition to the common effective crisis communication methods, crisis communication theory Situational Crisis Communication theory (Coombs, 2007) will be implicated to this research. Data collected in this thesis and the results rose from it will be compared to the SCCT theory. Concepts and models of the theory will be used with care to analyze the findings from the existing data. The theory is used only for its relevant sections considering this research.

According to the theory crises can be categorized into three crisis clusters (Appendix 1) and matched to response strategies (Appendix 2). Since Facebook was attacked by hackers and it did not practically cause the breach by itself, it can be said that Facebook belongs to the 'victim' crisis cluster with September 2018's data breach case. However, according to the SCCT theory, victim cluster possesses 'mild reputational threat', which often is not the case with large data breaches, especially when individuals' outside an organization are affected. Therefore, Facebook's data breach from September 2018 can also be categorized as 'preventable', since the company has faced large data breaches also in the past. This is also because the data breach rose from an error in

Facebook's system, which allowed hackers to get access to users' accounts and the private data included in them. With a preventable cluster, the severe reputational threat is often possible for the organization. Thus, this research will apply both victim and preventable crisis clusters and the response strategies matched to them when analyzing Facebook's September 2018 crisis communication.

When moving into the crisis response strategies (Appendix 2), the possibility of categorizing Facebook's crisis case into two different categories either limits or extends the possibility of using crisis communication response strategies of SCCT theory as a benefit. To help analyze which crisis response strategy would benefit the Facebook case the most according to SCCT, it is good to use the guidelines for crisis response strategies by the SCCT theory (Appendix 3). As mentioned in the literature review, the response strategies can decrease the negative impact of a crisis and help to repair organizational reputation as well as shape organizations position in a crisis situation. Based on the SCCT theory, at least one of the primary crisis response strategy, 'deny', is not relevant for Facebook, because they were the ones who had the ability to spot the data breach. This means that Facebook should according to the SCCT theory either aim for diminishing strategies (excuse, justification) or/and rebuild strategies (compensation, apology). This situation is manageable, because according to the crisis response strategy guidelines (Appendix 3: Number 8.), 'deny' strategies should not be mixed with 'diminishing' and 'rebuild' strategies because it erodes the positive effect of the crisis communication.

Concentrating on the usage and benefits of 'diminishing' and 'rebuild' strategies, SCCT theory's crisis response strategies suggest using them in a certain way. The 'diminishing' strategies should work best when matched to crises where the organization had the minimum amount of crisis responsibility and had some history with similar crises or prior negative relationship reputation (Appendix 3: Number 3., victim crises). The 'diminishing' strategies should also be used when the crisis is an accident and there is no history with similar crises and the relationship reputation is either positive or neutral (Appendix 3: Number 4.).

With 'rebuild' strategies, the crisis should have low attributions of crisis responsibility (accident) and the organization should have no prior history of similar crises and/or negative prior relationship reputation (Appendix 3: Number 5.). Also, when the organization has a strong attribution for crisis responsibility (preventable crises),

‘rebuild’ crisis response strategies should be used regardless of prior crisis history or relationship reputation. (Appendix 3: Number 6.).

Considering the crisis communication options, which the SCCT theory offers, it is good to note that Facebook does have a prior history of similar data breach crises (discussed in Findings and analysis in more detail). Prior relationship reputation with stakeholders is not that simple as Facebook is still one of the biggest social media platforms. These facts, however, do not affect the crisis response strategies, ‘diminishing’ and ‘rebuild’, since they both should be suitable (according to the SCCT theory) for the type of crisis Facebook regardless of their history.

To summarize what the SCCT theory suggests for ‘victim’ and ‘preventable’ type of crises, the table below will show what would be the most effective way to proceed with common crisis communication theory (SCCT) for Facebook’s case:

Crisis cluster	**Response strategy**	**Explanation**
Victim	**Diminishing strategies** (Excuse, Justification)	**Excuse**: Minimizing organizational responsibility by denying intent to do harm or claim an inability to control the crisis causes **Justification**: Minimizing the perceived damage caused by the crisis
Preventable	**Rebuild strategies** (Compensation, Apology	**Compensation:** Offering money or other gifts to crisis victims **Apology**: Indicating that the organization takes full responsibility for the crisis and asking for forgiveness from the stakeholders

Table 4 Suggestions for matching the crisis cluster with crisis response strategy according to the SCCT theory

According to the SCCT theory, while maintaining consistency, a mix of these primary crisis response strategies should be the most beneficial crisis communication strategy for Facebook’s 2018 September’s case. Secondary crisis response strategies are not taken into consideration with this research, because the guidelines for crisis response

strategies do not take them into account and they are not relevant for the crisis communication Facebook used in their September 2018's data breach case.

4. Findings and analysis

4.1. Structure of findings and analysis

Findings and analysis of this thesis are structured into three different sections. The three sections are divided based on three dates (Sept 28, Oct 2, and Oct 12, 2018) when Facebook's published initial crisis communication messages (B1, B2, B3, F1, T1, T2, T3, T4). Sections include Facebook's own crisis communication presented and the response by the media (V, A). In other words, the media's reaction to Facebook's crisis communication will be taken into consideration with additional comments from individuals (included in media posts). The third section also includes additional information about Facebook's state with possibly changed stock prices and user amounts. In more detail, the first section handles data published during Sept 28, 2018 – Oct 1, 2018, the second section handles data published during Oct 2, 2018 – Oct 11, 2018, and the third section handles data published on and after Oct 12, 2018. Sections are divided based on Facebook's own initial crisis communication.

4.1.2. Facebook's prior crisis history and its effects on crisis communication

It is good to note that Facebook already faced one major data breach during 2018, which was brought up in multiple data sources. In brief, a company called Cambridge analytica gained access to private information of initially over 50 million Facebook users. The number of users affected later on increased to over 87 million user accounts. It was found out that the company was hired by the President of the United States, Donald Trump, to identify personal information about American voters and influence their behavior (Granville, 2018; Meredith, 2018). This data breach crisis might have an effect on Facebook's crisis communication and the stakeholder's response during their September's 2018 case.

4.2. Section 1: Facebook's first response to the data breach crisis

4.2.1. Facebook's first crisis communication messages

Based on the data collected (Appendix 3), Facebook first tackled the data breach crisis through their own blog, Facebook Newsroom, on Friday, September 28th in 2018. B1 was the first message Facebook sent for the public two days after the engineering team had discovered the data breach on Wednesday, September 26th. The process of crisis communication was started by the VP of Product Management, Guy Rosen, who posted a security alarm blog post with a headline ''Security update''. The blog post was also shared through Facebook's own Twitter account (@facebook) to notify the public about the crisis also through social media. Blog post's key message for its readers was to apologize from the users of Facebook and mention that Facebook is taking this issue very seriously and it is taking steps in order to find out who's behind the attack and what is going to happen next. Facebook explains in the first blog text what they have done so far (fixed the vulnerability and informed law enforcement, reset the access tokens for the 50 million accounts affected and for additional 40 million accounts, closed the 'view as' feature), and share's steps for the users affected in the crisis (i.e. checking from the Help Center how to continue if there are any problems with logging back in). Facebook's blog post by Guy Rosen emphasizes that attack was caused by multiple and complex issues in their code, which stemmed from a change made in Facebook's video uploading feature in July 2017.

In addition to Guy Rosen's text, B1 was later continued by VP of engineering at security and privacy Pedro Canahuati, who explained additional technical details related to the case. He explained how the hackers got access to users' accounts by using three bugs in Facebook's system, reviewed what has been done and defined concepts related to the data breach ('view as' feature and process of getting the access tokens through video uploading feature system mistake made in July 2017). In addition to the B1, Facebook increased their communication for the public through sharing the post in social media. T1 and T2 were published for the Twitter followers of Facebook to notify users about the information considering the crisis. T1 and T2 only included short notification for the readers about the crisis and the blog post (B1), which includes more information. In addition to this, company's CEO Mark Zuckerberg also published a Facebook post about the crisis (F1), where he listed what has happened similarly to

Rosen's text (B1) and reminded the stakeholders about Facebook's constant vulnerability for these types of crises.

F1 also mentions that regardless of their actions on protecting the users' information and fixing the technical issue in the system, these crises should not happen, and the company will be focusing on their security more in the future. This message is also emphasized in a recorded interview with Mark Zuckerberg (V1), where the CEO of the company again mentions that they face constant digital attacks. In CNBC's interview on Sep 28th, 2018 (V1), Zuckerberg also states that Facebook needs to do more to prevent these kinds of crises from happening in the first place. Zuckerberg does create a more positive picture of the company by ensuring that the company is currently focusing on taking more responsibility for the safety of the Facebook community. CEO emphasizes that the investigation is ongoing and taken very seriously and that the stakeholders will be informed as soon as they get more information.

When comparing Facebook's initial crisis communication messages to the SCCT theory and common effective crisis communication methods, Facebook managed to do many things right, but also many things wrong in their messages. First, Guy Rosen did apologize from their users (B1), which matches the SCCT theory's ''preventable'' crisis cluster and the 'rebuild' crisis response strategy (Table 4). However, CEO Mark Zuckerberg said in his Facebook post (F1) that the company faces ''constant attacks like this''. Thus, Facebook was also using a bit of 'justification' in their crisis communication to minimize the seriousness of the crisis. Regardless of this, F1 added a link to B1 saying that it contains more information about the crisis. Therefore, F1 and B1 were linked to each other for stakeholders to reach all available information from the company. Through linking the texts together and including similar information to both F1 an B1, Facebook maintained consistency with crisis communication without unnecessary confusion.

When considering the common characteristics of effective crisis communication (Informative, Transparent, Spontaneous, Targeting, Instant), at this point, Facebook does qualify for part of these characteristics with their first messages about the crisis (B1, F1, T1, T2 and Zuckerberg's interview for CNBC, V1). T1 and T2 were more meant to share the actual crisis messages to a larger audience instead of providing any new information. Thus, they were not providing information, but they were spontaneous and instant and targeted to Facebook's Twitter followers. B1 and F1 were also targeted to the audience of Facebook's users but lacked informativeness, transparency, and

instant messaging to some extent. Facebook itself discovered the crisis already two days before the crisis was published but decided to share the information after they had discovered more information. This is indeed a good decision when considering the amount of information and transparency of crisis communication. Still, B1 announced that many aspects of the crisis have not yet been discovered, including who did it, why they did it, what was stolen, what was the location and where were the hackers. F1 also mentioned that more information is needed, but the stakeholders will be informed when information is updated. B1 did defend the position of the company by saying that they just started the investigation, which was most likely supposed to justify the decision of not sharing more information. Also, B1 emphasized that immediate action has been taken, which ensures the stakeholders that repairing the damage is happening.

It is clear, that Facebook has faced a data breach crisis before. Even if the first messages of the crisis communication lacked a lot of crucial information of the crisis, Facebook knew that the stakeholders of the crisis must be informed quickly due to the threat of crucial personal data. Facebook did explain briefly what they already know and what they have already done in order to reduce the possible panic of the audience and apologized from the stakeholders. Facebook also used some justification (F1: Zuckerberg mentioned that they are constantly facing crises like this), which most likely helps the company to lower its viewed crisis responsibility by the stakeholders. In addition to this, Facebook ensured their audience that they are currently investigating the case in more detail and will take immediate action to protect any possible additional user accounts that are found to be harmed by the hackers.

To summarize, Facebook did use two of the suggestions of SCCT theory's guidelines for the crisis response strategies (justification, apology). and with 'spontaneous', 'targeting' and 'instant' characteristics of effective crisis communication (based on the literature review). Transparency and informativeness were included partly in the first messages, but crisis communication of the data breach crisis lacked still a lot of crucial information about the crisis. Spontaneous, targeting an instant showed through the multiple media used (Facebook, Blog, Twitter) and through the promise of providing more information as soon as the company gets it (B1). Next, the analysis will focus on how the decisions considered Facebook's own crisis communication affect the response of the media.

4.2.2. The first response to Facebook's crisis by the media

When Facebook announced the crisis on September 28th in 2018, multiple media immediately reacted to it (A1, A2, A3, A4, A5, A6, A7, A8, V2, V3) and published content about the crisis. In other words, the first week after the crisis was published (Sep 28 – Oct 1) by Facebook was the busiest when it comes to the responses of different media to Facebook's data breach announcement. The responses of the media will be analyzed in two parts, which are the negative and the positive part. This means, that articles and videos, which took Facebook's crisis messages more negatively, will be looked at separately of the articles and videos, which took Facebook's crisis messages more positively. After this, it will be analyzed whether Facebook could have done something different with their crisis communication when they first announced the crisis.

4.2.2.1. First section: positive response from the media

From the data sources posted after Facebook's announcement on September 28th to October 1st, 2018, the remaining 3 website articles (A2, A4, A8) and one video (V3) included content about Facebook's crisis, which was completed without showing a clear negative opinion about the company. Articles posted on September 28 (A2, A4) included assumedly also a lot of basic facts about the crisis itself, as well as one of the videos (V3), even if it was posted later on October 1st. A8 was a continuing article for A2 with the same authors and it focused on the topic of what is going to happen next after the major data breach. Out of A2 and A4, A2 focused the most on the basic facts of the crisis published by Facebook before moving into analyzing the company. Both articles did also include parts of interviews made with Mark Zuckerberg and Guy Rosen, where the company stated again that they were still not aware of who the attackers were and where the attack was located. Facebook had however started already working with the FBI and knew, that (according to A2 and A8) no credit card data or passwords were stolen, but third-party apps (apps which allow the user to log in through Facebook) might have been affected by the crisis.

When analyzing the first positive data set, V3 was an informing video about the case its viewers with positive music background, but A2, A4, and A8 also included argumentative points, which shows that company's reputation had not yet suffered in

their opinion. For example, A2 and A8 pointed out also Facebook's previous setbacks during 2018 but still stated that none of these crises has shaken the confidence of global 2 billion Facebook's users. These two articles were, however, in general, more neutral than positive when considering the media reactions about for the company's communication. A2, for example, included a comment of concern by a security expert Jake Williams, who was worried that other Facebook apps or third-party apps were damaged also during the crisis and continued it by adding Rosen's comment received late on Friday night (Sep 28) that they might have been. Regardless of this, A2 brings up a previous larger data breach crisis of Yahoo!, and states that it cannot yet be known how serious the attack was before the company knows who the hackers were.

In addition to this, A2 includes a comment by Wedbush analyst Michael Pachter, who mentioned that the most important thing in the crisis is that the public founds out the seriousness of the crisis (whether a state was involved in the crisis) and that as a user, he wants Facebook to protect his data and let him know when it is compromised. It is also good to note that A2 also includes a defensive comment for Facebook's situation by a professor at Johns Hopkins University, Thomas Rid, who states that the hackers were most likely not connected to any nation-state. According to Rid, the hackers were most likely criminals or spammers with very little or none sophistication, since 50 million random Facebook accounts are not interesting for any intelligence agency. In other words, A2 does not judge the company before all possible information is available and as long as the company keeps protecting users' data. A9 continued this by stating that the 'waiting game' has started, as the information has not yet been published. Otherwise, A8 includes all the same facts and comments as A2 does, which shows that it is only continuing A2 and possess the same neutral attitude towards Facebook as A2.

The most positive and hopeful of all the positive or neutral sources was A4. Regardless of the misleading negative headline of *Why Should Users Trust Facebook? It's a Hard Question for Mark Zuckerberg to Answer, the* article does specifically compliment Facebook's improved crisis communication about their security issues. First, A4 explains in brief what the case is all about and discusses the fact of how Facebook's executives had again faced a 'painful' news cycle. The article explains also that even if Facebook's still unaware of multiple factors considering the data breach, investigation with the FBI has been started. Also, Zuckerberg's comment in the article, about how the Facebook's security is an 'arms race' against people in the community who want

to steal information followed by comments on how Facebook has tackled big crises before, shows that the article believes in the company.

About the crisis communication A4 states how Facebook has successfully improved its transparency for the press and the users by informing the crisis this soon after the breach was discovered. In addition, according to A4, the company's apology shows 'humility' and proves that the company is able to put the community of 2 billion users under 'one roof'. In addition to this, A4 mentions that Zuckerberg and Rosen have shown determination even if it means to tell the users of Facebook that their data has been endangered. This shows, that A4 article does believe in the company. At the end of the A4 article, it is also stated that roughly 90 million people will face only ''a small inconvenience'' of being logged out from their accounts and adds Zuckerberg's comment of the Facebook's need to ''do more'' for the security.

4.2.2.2. First section: negative response from the media

Unfortunately for Facebook's multiple media took the news about the data breach as a negative effect on the relationship between the media and the company. Data sources A1, A3, A5, A6, A7, and V2 all explained what Facebook had published about the crisis, but also showed, that they were more disappointed than pleased with Facebook actions. Unlike the more positive data sources, the more negative data sources brought up the mistakes in Facebook's history of crises and in their current crisis communication. Facebook was widely judged by their lack of information shared for the public and the decreasing trust towards the company was brought up multiple times.

In more detail, all articles chose to present Facebook in a more negative light rather than enhance the positive relationship between the media and the company. For example, A1 mentioned Facebook's already bad history with similar crises and stated that the news could not have come at a worse time. In addition, A1 talked about the system bugs Facebook had as ''awkward for a company that takes pride for its engineering'' and brought up a comment by critics saying that the attack Facebook now faced is a sign that the company has yet to come to terms with its problems. According to a commissioner of the Federal Trade Commission Rohit Cobra (A1), data breaches don't just violate user privacy. Instead, they create enormous risks for the economy and national security. A1 also reminds readers about the critique Facebook has faced

due to its history of being slow to notice security issues in their vast platform. Also, even if Facebook's efforts to increase their security through improved systems, A1 states that Facebook's recent data breach was ''just a reminder'' of how difficult it is to entirely secure a system of 2,2 billion users globally connected to Facebook's other or third-party services. Lastly, A1 criticized how it is easy to find detailed reports about the data breach through Twitter and Google searches, Facebook remains as the one place where they were difficult to find.

As A1 showed lack of trust through the text towards Facebook, A5 and A6 continued by adding the unfortunate information about Facebook's already low (A5) stock prices, which had dropped again after the crisis. A6 also brings up the fact that the crisis came at a time of significant strife for Facebook, which is already facing criticism over ''foreign election interference, the flow of misinformation, hate speech, and data privacy''. These statements do not increase the company's reputation, as well as the fact that A6 accused Rosen about ''not providing any details'' and saying ''only that the attack seemed broad'' doesn't increase the image about transparent crisis communication by Facebook. In addition to A5 and A6, V2 also brings up to the trust issue towards the company as ''another major setback for Facebook, the social media giant already under fire for not protecting users' private information''. Accusingly, V2 also shows only a part of Zuckerberg commenting about their previous crisis in April 2018 at the Congress, saying that they might not be able to fully stop everything, and continues to shame the company through an interview with people picked up from the streets.

When V2 interviews people picked up from the street, three people were interviewed. The first person interviewed said that so much has gone down at Facebook, which affects her trust towards the company decreasingly. The second person to be interviewed mentioned that one would think that Facebook would have some ''security walls'' to prevent these crises and the third person's opinion was to not trust any similar companies fully because of the threat of being hacked. V2 also brings up Facebook's history of similar crises again by mentioning that it's been tough two years for the company who has also been investigated by the FTC and FBI after the Cambridge analytica case. V2 shows a clip of Mark Zuckerberg from April 2018, where he states that Facebook is run by him and he takes full responsibility, and after mentions that Facebook is again struggling to retain the trust of its users.

When moving back to the articles, A3 and A7 showed their negative attitude towards the company in a gentler way compared to the previous data analyzed (A1, A5, A6,

V2). A3 was providing a set of guidelines and answers for users on what they should do now that the crisis has been published. A3 also brings up the ''rocky year'' Facebook has already had and the fact that the company is ''scrambling'' to get its users' trust back. A7 also mentions the ''stemming loss of public confidence'' and emphasizes also the fact that a lot about the crisis ''still remains as a mystery''.

To summarize, many data sources stated their lack of trust towards a company which has already faced multiple challenges during the past year. Lack of transparency and information was also brought up in the negative sources. However, the negative response might also be caused by the crisis history of Facebook and by the fact that single mistakes a company makes might turn into more significant when it faces a major setback, instead of just mistakes made in Facebook's crisis communication.

4.3. Section 2: Facebook's update on the security issue

4.3.1. Facebook's update about the September 2018 crisis

On October 2nd, 2018, Guy Rosen published another blog post to Facebook's newsroom (B2), which was also later shared at Facebook's Twitter account (T3). Twitter post was only again sharing the second blog post by Facebook without sharing any extra information. The blog post instead was updating the security issue Facebook in the previous week. At the beginning of the blog post, Facebook stated their will of providing the update about the crisis for the stakeholders, and briefly recapped what happened in Facebook's September data breach and that they had already fixed the vulnerability. Facebook also answered the question of whether the other Facebook apps or the third-party apps were affected by the crisis by stating that no evidence has been found on that issue. The blog post also mentions that they are currently building a tool for all developers, who are using Facebook as part of their logging system (Facebook SDK), to help them log out all accounts that might have been damaged during the crisis. In the end, Facebook again emphasizes how important security is for them and apologizes once again from the stakeholders of the crisis. The company also again promised to update the public as soon as they get more information about the crisis.

With Facebook's second set of own crisis communication, many things were missing again. Facebook is currently being spontaneous and targeting with their crisis

communication as they are providing information as soon as they know a little bit more and they are targeting their messages to specific audiences (B1 for the users, B2 for the developer's using Facebook SDKs. However, as the more negatively reacted media mentioned previously, transparency and informativeness were still missing mostly in Facebook's second blog post (B2). Facebook did not provide any additional information about the hackers and their reasons behind the attack, about the location where the attack happened or about what personal information of the users has been threatened by the crisis. Facebook did not even state that they were still unaware of these aspects of the crisis in B2, which might awake more questions among the public.

When comparing Facebook's second blog post to the SCCT theory's crisis response strategies and the crisis response guidelines (Table 4), Facebook again used apologizing from the rebuild strategies. Facebook also offered help for its developers, but it does not qualify as compensation since the developers did not benefit directly from the helping tool Facebook provided. Other response strategies according to the SCCT theory were not used in B2 or in T3.

4.3.2. The second response from the media

After Facebook updated its data breach crisis on October 2nd, the media responded again. From the data set A9, A10, A11, and A12 were published after Facebook announced the update on their data breach crisis. It can be said, that there were fewer media articles to be found after B2. This might be because the ''shock'' of the crisis had already past or because Facebook did not post a lot of new information considering the crisis.

4.3.2.1. Second section: positive response from the media

Again, part of the media took Facebook's second set of crisis communication more positively than other media. From the second section's data set, A10 and A12 showed more hope and trust towards the company. Both articles recapped the crisis but also moved quickly into a deeper conversation about the Facebook situation. However, out of the two articles, A12 was the more neutral one. In A12, attitude towards the crisis and Facebook was more pensive, since the article was discussing different options what might happen to Facebook if certain things happen. A12 did list multiple things that are still a mystery about the crisis but also added what is already known. In

addition, A12 explained that things might go very wrong for Facebook if, for example, the hackers chose to publish all the data (i.e. private messages) they possibly have stolen from the company. A12 also guessed that hackers could also be blackmailers for example to political figures or try to steal their account information in order to have an effect on possible elections.

Regardless of this, A12 continued the article by saying that none of this might happen. It is also possible that no private information has been accessed or stolen and the hackers were just ‘’playing around’’. A12 also hopefully stated that Facebook will soon answer the most asked questions all around the world. After this, A12 did continue with the guessing by saying that even if this crisis has gotten less attention than the previous crisis Facebook had in April 2018, it might affect more people. A12 also brings up the importance of trust and the major issues it may cause to lose it for a company like Facebook. However, A12 does not despise or show any other negative opinions towards the company in the article. Instead, A12 leaves Facebook’s situation open and in addition to the worst possible scenarios reminds the public that it is also possible that no harm has happened for people’s personal information.

A10, on the other hand, focuses highly on Facebook’s crisis communication instead of repeating the crisis itself. However, the article focuses on all Facebook’s crisis communication it has published considering the crisis happened in September. At the beginning of the article, A10 praises Facebook for improving their crisis communication. In the headline, A10 mentions that Facebook ‘’rapidly’’ announced their crisis and in the text that Facebook has ‘’taken a page’’ from its recent crisis communication in previous crises. The article also mentions how Facebook has informed what the company has done for the crisis and what will be done to repair the situation of the company. To support this, A10 gives many citations directly from Facebook’s crisis messages published in their blog. In addition to this, A10 adds a comment from the principal of Bospar PR and crisis communication leader Curtis Sparrer, who praises Facebook for finally learning from their mistakes in crisis communication. Sparrer states in his comment that instead of waiting for months or years, Facebook chooses to alert the public in the very early phase of the crisis. A10 continues that a transparent and well-structured crisis communication may help the organization a lot when repairing the trust between the company and the stakeholders. Especially when the crisis communication is fast.

4.3.2.2. Second section: negative response from the media

As usual, part of the media did not respond to Facebook's crisis communication in a positive manner. Out of section 2 articles, A9 and A11 had a negative attitude towards Facebook after Facebook had posted their second blog post about the crisis. Articles A9 and A11 both had their suspicions towards the company and for the information, Facebook is sharing about the crisis.

Article A9 has its main focus on Facebook's ''muddy response'' for the data breach crisis. At the beginning of the article, A9 points out that the users of Facebook have been frustrated, because of the lack of information considering the Facebook crisis. The article also brings up the fact that data breach investigations have always taken a lot of time, but because of the General Data Protection Regulation (GDPR), companies must act quickly when announcing a possible cybersecurity issue. However, A9 mentions that this does not mean that the company will publish any details in the early stages of the crisis and the more detailed information might take some time. As head of the cybersecurity practices at Greenberg Traurig Paul Ferrillo states, it is difficult for any company to produce a ''perfect notice'' about the cybersecurity crisis, but the GDPR requires companies to make the public aware about the cybersecurity crisis within 72 hours from the discovery of the crisis.

A9 also mentions Zuckerberg's comment about the fact that Facebook's crisis was specifically a complex cybersecurity crisis. However, A9 does indirectly state that Facebook is struggling with its crisis communication by stating that also other companies have struggled with the ''changing narrative that plays out in the public eye''. This is also a critique of other media, but A9 does not go any deeper with it. Instead, A9 continues by stating that regardless of Facebook's efforts to the security of the company, it has faced privacy and security scandals. According to A9, consumers will most likely not be forgiving for these types of crises, and that according to Data Protection Commission (GDPR), it is worrying how Facebook is unable to clarify the nature of the breach or the risks for individual users at this point of the ongoing crisis. This shows, that A9 does not have a strong trust at Facebook's crisis communication at this point. A9 concludes the article by stating also an important fact that the bad crisis communication might be the new norm of crisis communication about data breaches, under the new GDPR.

A11 from section two data set moves its focus to the CEO of the company: Mark Zuckerberg. A11 starts the article by saying that Zuckerberg is facing a ‘’major public reckoning’’ after the data breach when Facebook is increasing the number of company crises. The article brings up the fact that it is not the first time in Facebook’s history when the CEO is being questioned, but this time the situation does look bad due to the three flaws in Facebook’s, which the hackers managed to exploit. A11 continues this argument by adding a strong argument by Pivotal Research Group analyst Brian Wieser, who said that the hack is just a sign of a much bigger problem of the badly managed company. A11 continues by stating that Facebook’s profitability and popularity have hidden the concern around the company, but the track record of Facebook should concern for example investors. Wieser also argues that Facebook should investigate its problems properly, and if it is the CEO’s or COO’s responsibility, the company might want to consider other persons as their executives.

The lack of trust towards the company also shows in A11 by explaining that many things about the crisis still remain unknown. Also, CFRA analyst Scott Kessler’s comment (A11) on how the recent data breach only increases the concern towards the company and its management, does not increase the positive image of the company. In addition to this, A11 mentions that the crisis might turn into worse and questions whether Facebook has done enough in order to secure it's over 2 billion users’ data. Also, A11 talks about Zuckerberg’s plans on increasing the security forces as areas that are already heavily invested. This is continued by A11 talking about the risk of Facebook receiving heavy fines due to the GDPR, and arguing that distrust towards Facebook’s handling of user data has already started when the company was founded. At the end of A11, a comment from eMarketer analyst Debra Aho Williamson about how the recent crisis will definitely not improve Facebook’s image, especially when the crisis comes at a worst possible time for a company that is already suffering from recent crises.

4.4. Section 3: Facebook’s final update about the data breach

4.4.1. Facebook’s final crisis update

Facebook posted its last blog post about the crisis on October 12, 2018, where it published the results of their two-week investigation considering the data breach crisis (B3). The post was again shared in Facebook’s Twitter account without any additional

information about the crisis (T4). In the blog post itself (B3), Facebook stated that it has been working ‘’around the clock’’ in order to investigate the security issue they discovered and fixed on September 28th. The company still keeps investigating some smaller-scale attacks, but now it announces how did the company discover the attack and how many people are actually affected by the crisis and how.

In B3, Facebook quickly recaps the crisis before explaining how the crisis was discovered inside the company. According to Guy Rosen (B3), the company noticed an unusual spike in their activity on September 14th in 2018. That is when the investigation started and on September 25th, the company defined the spike as an actual attack and identified the vulnerability in the Facebook code. The attack was closed in two days as well as the vulnerability was fixed, and the users’ accounts were protected. Now, the company announced that fewer people were affected by the crisis then it originally stated. Out of the initial number of 50 million user accounts affected by the crisis, only 30 million accounts actually got their tokens stolen.

B3 explains in the blog post clearly how did the hackers get access to users’ accounts. According to Rosen, the hackers used an automatic technique, which allowed them to move from one account to another, totally up to 400 000 accounts. Eventually, the hackers were able to use a portion of these accounts’ friendslist to access around 30 million people. Out of these 30 million people, hackers got access to 15 million users’ name and contact details (email, phone number) and 14 million users’ name and contact details as well as other details included in the accounts (i.e. birthday, language, relationship status, religion, hometown, self-reported current city, education, device types used in Facebook, tags, workplace, etc.). For the remaining 1 million user accounts, the hackers did not access any information. In the end, B3 gives instructions for users to use the Help Center if they want to know whether they were affected. Also, customized messages will be sent to the 30 million users affected, where Facebook will inform what information may have been accessed and the steps how users can help to protect themselves. B3 includes photos of how the customized message looks like and, in the end, adds that no other apps (Messenger, Messenger Kids, Instagram, WhatsApp, Oculus, Workplace, Pages, payments, third-party apps, or advertising or developer accounts) were affected in the data breach.

When comparing Facebook’s last update about the crisis to the common effective characteristics of crisis communication, the transparency and informativeness were especially improved, if they weren’t fulling the stakeholders’ expectations before. Also,

B3 was targeting its audience very clearly through giving instructions for the users' whose accounts might have been affected by the crisis. The blog post was also spontaneous as the company published and shared (T4) the data when it had it and it was instant when comparing for example to A10's comment about normally waiting Facebook's crisis communication for months or even years. However, even if the characteristics of effective crisis communication (based on the literature review) were filled, the information Facebook shared was relatively shocking when considering the amount and privacy of the information that got stolen in the data breach. This might have an effect on how the media is going to respond. Facebook also did not use any of the respond strategy suggestions (Excuse, Justification, Compensation, Apology, Table 4), which shows that Facebook chose to only share additional information about the crisis.

4.4.2. The final response from the media

As well as with the second set of the media responses, third section response amount is less than with the first section. From the data set A13, A14, A15, and A16 were published after Facebook's final crisis communication messages on October 12th in 2018.

4.4.2.1. Final section: positive response from the media

Out of the four data sources, A13 took a more positive attitude towards Facebook in the article. First, the article states three key points, where it states that the number of users was less than what was first announced, what information was stolen and from who and the fact that company published a website where users can check whether their account was affected by the crisis or not. The key points are followed by a video, where CNBC reporter states the current updated facts about the crisis and emphasizes that the new Facebook crisis information is not about a new crisis. In addition to this, the CNBC reporter praises Facebook for making a ''big push'' in order to be more transparent about their security issues and publishing the details about the crisis. The article (A13) also explains in more detailed what has happened according to Facebook in the crisis and ads Rosen's comment about the high importance of Facebook's users' security and being sorry for what has happened. A13 also adds as Facebook's defense a comment from the company saying that the FBI asked Facebook to not share the information about who the hackers were. In addition, regardless of A13 sharing the information about Facebook's decreased share price, the article states that Facebook

‘’discovered and disclosed’’ the crisis and is not showing signs of not trusting the company’s information or decisions.

4.4.2.2. Final section: negative response from the media

Three articles out of the third section data set, A14, A15, and A16, presented Facebook in a more negative light then A13. All of the three negative articles explained what Facebook had updated about the crisis and provided the information about how a user of Facebook can check whether their account was affected by the crisis. The negative attitude towards the company is mostly not direct in these articles, but it is hidden in the sentence and word choices of the articles, as it has been often within the previous first and second section’s negative articles.

First, A14 started the article with threatening news on how hackers could have ‘’exposed’’ some users private personal data. A14 continues by stating that Facebook has now shared the information the hackers took for the first time and mentions that even if the original 50 million was an incorrect amount, 14 million people still had ‘’sensitive’’ information accessed. A14 increases the negative image of the company by adding also a comment from privacy experts, who think that personal details might be as valuable and important as financial information for consumers and for criminals. In addition to this, a comment by the director of consumer privacy and technology for Consumers Union Justin Brookman states that for example people’s personal messages might include ‘’very sensitive information’’, which Facebook cannot replace similarly to for example credit card numbers. A14 also adds a threatening comment from Casey Oppenheim (founder of the data security firm Disconnect), where she states that if the hackers had access to the user's account, they could have ‘’basically impersonate’’ the user and access to anything a user does in Facebook. Oppenheim also comments in the article that big data companies, such as Facebook or Google, do a very good job of convincing people about their security, but often that is not the case.

Lack of trust towards the company also shows in A15, which also immediately brings up what information of users has been taken. A15 then, like other articles, explains what Facebook has now updated about the crisis, but also brings up a possible fault in Facebook’s crisis management. A15 asked Facebook whether it is going to give some compensation for the users affected as it is common with data breach crises but received an answer from a spokeswoman saying ‘’not at this time’’. A15 also brings up, in addition to the details on how the hackers got the information from one account to

another, the fact that the possible outcomes of the crisis might be way worse than first expected. Similarly, A16 provides the details (what has happened and to how many) about the crisis and suggests that if a user has not yet started using a password manager or two-factor authentication, now would be a good time to do that. About the lack of trust towards Facebook, A16 also brings up the fact that the company was already struggling to regain its users' trust, and now, 30 million users' personal data has been exposed.

4.4.3. Reputational and financial damage caused by the crisis for Facebook

As mentioned before, the attitude (positive vs. negative) of a data source can depend on the very smallest details. As the findings and analysis show, the positive data sources did not all praise Facebook as a company or Facebook's crisis communication during the data breach. Instead, many articles focused on not to judge the company before the information has been released. Also, many data sources brought up the fact that this might happen for a big data company, but the company is taking actions in order to increase security. In addition, the increased transparency and instant messaging about the crisis by Facebook often got most of the positive feedback. On the other hand, a lot of the negative articles tried to bring up Facebook's prior negative history with similar crises and tried to make the facts about the crisis sound threatening for the readers. In addition, in contrast to the positive articles, negative articles blamed Facebook for not being transparent enough. These statements about a company that is already facing difficulties with the trust of its users, might cause both reputational and financial damage for the company.

When considering the financial reputation of Facebook after the crisis, it is difficult to tell how much the crisis for example cost for the company. Many articles speculated the amount that the company might have to pay fines under the GDPR, but according to A9, the amount was threatened to be over 1 billion dollars. When it comes to the stock prices of Facebook, on September 27th in 2018 the stock price in US dollars was 168,84 and approximately one month later on October 29th in 2018 the stock price was 142,09 US dollars. The scale had small peaks on the way but overall, Facebook's share price dropped according to Yahoo! Finance on April 4th, 2019 (search word: Facebook stock price). On April 4th in 2019 at 9 PM (Finnish time) the stock price was 176,16 US dollars (Yahoo! Finance, Facebook stock price, 2019).

Exact numbers are more difficult to present about the reputational damage the data breach caused by Facebook, However, The Economic Times (2018) published an article on December 31st in 2018 stating, that in a survey conducted in December 2018 by a company Toluna, 40% out of 1000 people nominated Facebook as the company they trust the least with users' personal information. Regardless of this, Facebook still remains as the most widely used social network and it had in 2018's third quarter 2,27 billion active monthly users and in the fourth quarter 2,32 billion monthly users (Statista, 2019). This statistic shows, that Facebook monthly user amount actually increased after the third quarter. Thus, it seems that even if the trust has decreased towards the company, it did not affect the user amount of the social media giant, Facebook.

5. Discussion and conclusions

5.1. Main findings and conclusions

When considering the main findings of this thesis, it is good to revise the research questions:

1. Do common effective crisis communication methods apply in a modern data breach situation?

The answer to the first research question is yes, they do apply. As mentioned previously, spontaneous, instant, targeting, transparent, informative are considered, based on the literature review, as commonly known effective characteristics of good crisis communication. Based on the data and the findings section, it can be said that these characteristics are as expected from data breach crises as they have been from the traditional crises. Many data sources brought up (either positively or negatively) directly the need for transparency, informativeness, and instant messaging when considering the crisis communication in a data breach situation. This all eventually is linked to the trust of the company, which is increased through these certain characteristics of effective crisis communication. Spontaneous characteristic is also needed, as many articles mentioned that they will inform the public as soon as more information is published, rather than hoping for a certain announcement schedule for

the crisis updates. In addition to this, data sources also always brought up Facebook's crisis messages about the guidelines how individual users should act in different phases of the crises (i.e. using the Help Center), which shows that targeting of the messages was appreciated by the media.

2. What, if anything, should be stressed in the guidelines for data breach crisis communication?

In data breach situations the most important characteristics to be stressed are instant messaging, transparency and informativeness. In a crisis situation, where the company faces a data breach, it is crucial to act fast and inform as well as possible the stakeholders of the crisis in order to avoid unnecessary reputational damage as soon as the data breach has been discovered. The instant messaging is not just required by the law (i.e. GDPR), but also by the stakeholders which the data breach crisis is affecting. If a company focuses on being transparent about the data breach crisis' events, informs the stakeholders and the public with all the necessary available information and does it fast, the risk of the crisis exposing to the public from another source is eliminated. As mentioned, data breach crises include the threat for very sensitive and secured data, and if the data is leaked for the public and the public finds out that the company was aware of the situation, but failed to announce it, trust between the stakeholders, public and the company will be majorly injured. Instant, transparent and informative crisis communication in data breach situations is also necessary for the repairing process of the crisis. Hereby the organization can inform the crisis stakeholders about what has happened and what they can do in order to minimize the damage (if it is possible) and show its interest towards taking the responsibility and helping the crisis stakeholders.

With the SCCT theory, the most important guidelines of the theory for crisis response strategy are to be consistent, apologize and take the responsibility both for the crisis and for the work to prevent a similar event in the future. In data breach situations, the communication from the company facing the crisis must come from clear sources and it should not include easily misunderstood information or contradictory from the company in any case, because the stakeholders must know that they are getting the correct information without being confused. Also, it is the company that faces the damage for not having the security to prevent the data breach, and the responsibility cannot be changed to any other party (based on the Facebook case). Thus, the

company should be the one to announce the responsibility and apologize for what has happened. One of the data sources also brought up the topic of compensation, which might be also in some cases useful in order to improve the overall company image after the crisis. Instead, excuse and justification seem to be unnecessary with data breaches, as they do not improve or worsen the response from the media.

Hence it can be stated that if anything should be changed from traditional crisis communication guidelines for traditional crises when moving towards the increasing issue of data breaches, it is the crisis communication theory. Most parts of the SCCT theory in this research ended up being incompatible or unnecessary with the modern data breach crisis type, which means, that either company should focus on another crisis communication theory when finding guidelines for data breaches or there should be a new modified theory for especially data breach cases. As discussed previously, the stakeholders of data breaches expect data breach crisis communication to be fast and include all necessary information, which is something that should be taken into consideration when building the possible theory for data breaches.

When it comes to the case and Facebook's own crisis communication results, Facebook should have either done something differently or the prior crisis history had its effects on the media responses. To recap the results from positive and negative responses from the media, it can be seen that more data sources from the whole data set were negative than positive. Out of the media reactions, 11 out of 18 data sources reacting to Facebook's communication were categorized as a negative response for the company (A1, A3, A5, A6, A7, A9, A11, A14, A15, A16, V2). The result shows, that for some reason, more media sources chose to show the distrust towards Facebook and present the company in a negative manner instead of accepting Facebook crisis communication decisions.

Considering Facebook's own crisis communication, the company did match with all the characteristic of effective crisis communication at some point during the first weeks after the crisis was published. Facebook's communication was, also according to many data sources, faster and more spontaneous than previously, targeting and transparent about the crisis. Informativeness was also increased in the updating blog posts after the company received more information about the crisis. From the SCCT theory's point of view, Facebook did use the apologizing and justification but did not use excuse or compensation, even if for example compensation was brought up by one of the data sources. Comparing these crisis communication choices to the number

of negative responses, it can be said that Facebook was most likely already having a bad image before the crisis in the media's eyes. Also, multiple data sources brought up the rough year with failed data security of the big data company Facebook, which proves that the much-talked prior crisis history does have the effect on how the stakeholders respond to data breach crises or crises in general. This means, that Facebook was already in the beginning in a difficult spot with its crisis communication, and it should have done something differently. However, because it is now clear that the media was expecting the characteristics listed before in Facebook's crisis communication, the things Facebook should have done differently do not have a lot to do with the crisis communication. Instead, the company is facing issues at the technical side of data security, and it is out from the topic of crisis communication.

5.2. Implications for International business

The global concern of data breaches and worldwide need for effective crisis communication methods in a fast and digitalized world are the most significant implications for international business of this thesis. Every organization restoring any private data must develop ways to protect their privacy, which is the reason why this research is important. Findings of this research present the relationship between a big global data company and the media, which is affected by the company's crisis communication. This can be then used as an example for all organizations globally, which are facing a data breach crisis. It is also good to note that Facebook's data breach was one of the biggest during the past decade, which makes it relevant to today's business world and the global threat of organizational crisis in the form of data breach. Finally, this research also uses only literature and data that has been published outside of Finland, which increases the international value of this thesis.

5.3. Limitations of the study

The first limitation of this research is the fact that this research is a bachelor's thesis conducted in a short amount of time and in a short amount of length. If this thesis was conducted with a larger scope considering the Facebook's case, it would have been possible to follow the effects of the major breach from a longer period time and in that way get more clear results of how their crisis communication worked. In this case, the maximum limit of the bachelor's thesis was reached, even if the case study took only the first two weeks into account after the crisis was published by Facebook.

Limitations of this research also include the lack of research made on data breach crises and crisis communication methods used in them. This might cause results biased to only one data breach case and one solution instead of giving instructions for effective crisis communication in all data breach situations. In addition to this, only one common crisis communication guideline theory was used in this research, which eliminates other theories of crisis communication including different guidelines for different situations.

A final limitation is the timing of this research. Facebook's data breach case is a relatively new phenomenon in today's business world, which causes a lack of academical research considering the case. This paper tried to optimize the relevance through as respected sources as possible, but it doesn't cover the value of academic and proved research information about the details in the case.

5.4. Suggestions for further research

For future research, it would be useful to focus more deeply into the developing of a crisis communication theory, which would have more implication for data breach crises than the already existing ones. Developing a theory would require more case studies and research on crisis communication in today's business world, but eventually it might be crucial for the efficient development of data breach crisis communication. Eventually, the research could also study more the effectives of post-crisis communication in data breaches, as it is also crucial for a company's image repairing.

When considering the case study about Facebook and data breach case studies in general, it would be useful that the data used in a similar research would follow the effects of crisis communication during a longer period of time, instead of the two weeks followed in this research. If more cases would be conducted using a similar methodology as this research, it would be possible to gather larger data for businesses to use when a data breach is threatening or happening for the organization. In addition, public opinions and comments about the crisis situation and the damage caused for the organization, in addition to the media comments, could be more widely observed, which would increase the value of the response analysis to a company's crisis communication.

References

Abraham, C., Tishler, A. (2005) 'Perceived Organizational Reputation and Organizational Performance: An Empirical Investigation of Industrial Enterprises' *ResearchGate* [Online]; 8(1):13-30 Available from: https://www.researchgate.net/publication/233662363_Perceived_Organizational_Reputation_and_Organizational_Performance_An_Empirical_Investigation_of_Industrial_Enterprises [Accessed 30 January 2019]

Acquisti, A., Friedman, A., Telang, R. (2006) 'Is There a Cost to Privacy Breaches? An Event Study' In: *Twenty-seventh International Conference on Information Systems (ICIS);* Milwaukee, Wisconsin, USA: 10-13 Dec [Online]; Available from: https://www.researchgate.net/publication/220268931_Is_There_a_Cost_to_Privacy_Breaches_An_Event_Study [Accessed 8 January 2019]

Andersen, P.A., Spitzberg, B.H. (2009) 'Myths and Maxims of Risk and Crisis Communication' In: Health, R. & O'Hair D. (1st ed.) *Handbook of Risk and Crisis Communication*. New York: Routledge. pp. 205–226.

Austin, L., Fisher Liu, B., Jin, Y.,(2012) 'How Audiences Seek Out Crisis Information: Exploring the Social-Mediated Crisis Communication Model' *Journal of Applied Communication Research* [Online]; 40 (2): 188–207 Available from: http://www.tandfonline.com/doi/abs/10.1080/00909882.2012.654498 [Accessed 27 December 2018]

Baker, W., Goudie, M., Hutton, A., Hylender, C.D., Niemantsverdriet, J., Novak, C., Ostertag, D., Porter, C., Rosen, M., Sartin, B., Tippett, P., Bosschert, T., Brohm, E., Chang, C., Dahn, M., Dormido, R., van Erck, B., Evans, K., Gentry, E., Grim, J., Hill, C., Kunsemiller, A., Lee, K., Lee, W., Long, K., Perelstein, R., Telemaque, E., Todd, D., Uzawa, Y., Valentine, J.A., Villatte, N., Beeferman, T., Dismukes, C., Goulding, P., Neal, C. (2011) '2011 Data Breach Investigations Report' [Online]; Available from: https://www.wired.com/images_blogs/threatlevel/2011/04/Verizon-2011-DBIR_04-13-11.pdf [Accessed 23 January 2019]

Benoit, W.L. (1997) 'Image repair discourse and crisis communication' *Public Relations Review* [Online]; 23 (2): 177-186 Available from: https://www.sciencedirect.com/science/article/pii/S0363811197900230 [Accessed 5 February 2019]

Breaux, R.W., Black, E.W., Newman, T. (2014) 'A Guide to Data Protection and Breach Response--Part 1' *Intellectual Property & Technology Law Journal* [Online]; 26 (7): 3–10 Retrieved from Aalto Finna [Accessed 7 February 2019]

Bryson, J.M. (2004) 'What to do when Stakeholders matter: Stakeholder Identification and Analysis Techniques' *Public Management Review* [Online]; 6 (1): 21–53 Available from: http://www.tandfonline.com/doi/abs/10.1080/14719030410001675722 [Accessed 30 January 2019]

Castillo, M. (2018) 'Facebook discovered "security issue" affecting 50 million accounts' [Online]; Available from: https://www.cnbc.com/2018/09/28/facebook-says-it-has-discovered-security-issue-affecting-nearly-50-million-accounts-investigation-in-early-stages.html [Accessed 21 March 2019]

Claeys, A.-S., Cauberghe, V., Vyncke, P. (2010) 'Restoring reputations in times of crisis: An experimental study of the Situational Crisis Communication Theory and the moderating effects of locus of control' *Public Relations Review* [Online]; 36 (3): 256–262 Available from: http://www.sciencedirect.com/science/article/pii/S0363811110000585 [Accessed 3 January 2019]

Clearfield, C., Tilcsik, A. (2018) 'How to Prepare for a Crisis You Couldn't Possibly Predict' *Harvard Business Review* [Online]; Available from: https://hbr.org/2018/03/how-to-prepare-for-a-crisis-you-couldnt-possibly-predict [Accessed 27 December 2018]

Cole, T.W., Fellows, K.L. (2008) 'Risk Communication Failure: A Case Study of New Orleans and Hurricane Katrina' *Southern Communication Journal* [Online]; 73 (3): 211–228 Available from: http://www.tandfonline.com/doi/abs/10.1080/10417940802219702 [Accessed 27 December 2018]

Coombs, W.T. (2014) *Ongoing Crisis Communication: Planning, Managing, and Responding* (4th edition) [e-Book] Available from: https://books.google.fi/books?id=CkkXBAAAQBAJ

Coombs, W.T. (2007) 'Protecting Organization Reputations During a Crisis: The Development and Application of Situational Crisis Communication Theory' *Corporate Reputation Review* [Online]; 10 (3): 163–176 Available from: https://doi.org/10.1057/palgrave.crr.1550049 [Accessed 27 December 2018]

Coombs, W.T. (1995) 'Choosing the Right Words: The Development of Guidelines for the Selection of the "Appropriate" Crisis-Response Strategies' *Management Communication Quarterly* [Online]; 8 (4): 447–476 Available from: https://doi.org/10.1177/0893318995008004003 [Accessed 2 February 2019]

Coombs, W.T., Holladay, S.J. (2005) 'An Exploratory Study of Stakeholder Emotions: Affect and Crises' In: Neal M. Ashkanasy, Wilfred J. Zerbe, Charmine E.J. Härtel (Volume 1) *The Effect of Affect in Organizational Settings (Research on Emotion in Organizations* Emerald Group Publishing Limited. pp. 263 – 280

Coombs, W. T. (1999) *Ongoing Crisis Communication: Planning, Managing, and Responding* Thousand Oaks, California, SAGE Publications

Coombs, W.T., Holladay, S.J. (1996) 'Communication and Attributions in a Crisis: An Experimental Study in Crisis Communication' *Journal of Public Relations Research* [Online]; 8 (4): 279–295 Available from: http://www.tandfonline.com/doi/abs/10.1207/s1532754xjprr0804_04 [Accessed 3 January 2019]

Cooper, A.H. (2002) 'Media framing and social movement mobilization: German peace protest against INF missiles, the Gulf War, and NATO peace enforcement in Bosnia' *European Journal of Political Research* [Online]; 41 (1): 37–80 Available from: https://onlinelibrary.wiley.com/doi/abs/10.1111/1475-6765.00003 [Accessed 6 February 2019]

Druckman, J.N. (2001) 'The Implications of Framing Effects for Citizen Competence' *Political Behavior* [Online]; 23 (3): 225–256 Available from: https://doi.org/10.1023/A:1015006907312 [Accessed 6 February 2019]

Edwards, B., Hofmeyr, S., Forrest, S. (2016) 'Hype and heavy tails: A closer look at data breaches' *Journal of Cybersecurity* [Online]; 2 (1): 3–14 Available from: https://academic.oup.com/cybersecurity/article/2/1/3/2736315 [Accessed 29 December 2018]

Egelhoff, W.G., Sen, F. (1992) 'An Information-Processing Model of Crisis Management' *Management Communication Quarterly* [Online]; 5 (4): 443–484 Available from: https://doi.org/10.1177/0893318992005004003 [Accessed 3 January 2019]

Eisenhardt, K.M. (1989) 'Building Theories from Case Study Research' *The Academy of Management Review* [Online]; 14 (4): 532–550 Available from: https://www.jstor.org/stable/258557 [Accessed 25 February 2019]

Fisher, J.A. (2013) 'Secure My Data or Pay the Price: Consumer Remedy for the Negligent Enablement of Data Breach' *William & Mary Business Law Review* [Online]; 4 (1), Article 7 Available from: https://core.ac.uk/download/pdf/73966375.pdf [Accessed 7 February 2019]

Freberg, K., Saling, K., Vidoloff, K.G., Eosco, G. (2013) 'Using value modeling to evaluate social media messages: The case of Hurricane Irene' *Public Relations Review* [Online] 39 (3): 185–192 Available from: http://www.sciencedirect.com/science/article/pii/S0363811113000386 [Accessed 4 February 2019]

Granville, K. (2018) *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens* Available from: https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html [Accessed on 1 April 2019]

Harvey, P., Martinko, M. (1982) *An Attribution Theory of Motivation and Emotion* [Online] Available from: https://www.researchgate.net/publication/232489124_An_Attribution_Theory_of_Motivation_and_Emotion [Accessed 2 February 2019]

Hayden, E. (2013) *Data breach protection requires new* [Online] Available from: https://searchsecurity.techtarget.com/feature/Data-breach-protection-requires-new-barriers [Accessed 7 February 2019]

Heath, R.L., Palenchar, M.J. (2008) *Strategic Issues Management: Organizations and Public Policy Challenges* [e-Book] Available from: https://books.google.fi/books?id=eLr114VLGksC [Accessed 29 January 2019]

Jaques, T. (2007) 'Issue management and crisis management: An integrated, non-linear, relational construct' *Public Relations Review* [Online]; 33 (2): 147–157 Available from: https://linkinghub.elsevier.com/retrieve/pii/S0363811107000185 [Accessed 4 February 2019]

Littlejohn, R. F. (1983) *Crisis management: A team approach*, New York: American management Association, Management Briefing.

McDonald, L., Härtel, C.E.J. (2000) 'Applying The Involvement Construct To Organisational Crises' *ANZMAC 2000 Visionary Marketing for the 21st Century: Facing the Challenge 5* [Online]; Available from: https://s3.amazonaws.com/academia.edu.documents/31158731/McDonal2.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1554478391&Signature=BglbEqbfRTABE2zq7mOrsky0jvA%3D&response-content-disposition=inline%3B%20filename%3DApplying_the_involvement_construct_to_or.pdf [Accessed 8 Januaru 2019]

Meredith, S. (2018) *Facebook-Cambridge Analytica: A timeline of the data hijacking scandal* [Online]; Available from: https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html [Accessed on 2 April 2019]

Milburn, T.W., Schuler, R.S., Watman, K.H. (1983) 'Organizational Crisis. Part I: Definition and Conceptualization' *Human Relation*s [Online]; 36 (12): 1141–1160 Available from: https://doi.org/10.1177/001872678303601205 [Accessed 2 January 2019]

Mishra, A.K. (1996) 'Organizational Responses to Crisis: The Centrality of Trust, In: Kramer, R.M. & Tyler, T. (eds.) *Trust In Organizations*. Newbury Park: Sage. pp. 261-287

Pearson, C.M., Mitroff, I.I. (1993) 'From crisis prone to crisis prepared: a framework for crisis management' *Academy of Management Perspectives* [Online]; 7 (1): 48–59 Available from: https://journals.aom.org/doi/abs/10.5465/ame.1993.9409142058 [Accessed 29 January 2019]

Penrose, J.M. (2000) 'The role of perception in crisis planning' *Public Relations Review* [Online]; 26 (2): 155–171 Available from: http://www.sciencedirect.com/science/article/pii/S0363811100000382 [Accessed 3 January 2019]

Perri, D.F., Perri, E.D. (2018) 'Acknowledging the "M" in MIS: Managing a Data Breach Crisis' *Journal of the Academy of Business Education Villanova* [Online]; 19: 9–32 Retrieved from Aalto Finna [Accessed 2 January 2019]

Pratt, M.G. (2009) 'From the Editors: For the Lack of a Boilerplate: Tips on Writing Up (and Reviewing) Qualitative Research' *Academy of Management Journal* [Online]; 52 (5): 856–862 Available from: https://journals.aom.org/doi/abs/10.5465/amj.2009.44632557 [Accessed 7 March 2019]

Reynolds, B., Seeger, M.W. (2005) 'Crisis and Emergency Risk Communication as an Integrative Model' *Journal of Health Communication* [Online]; 10 (1), 43–55 Available from: https://www.tandfonline.com/doi/abs/10.1080/10810730590904571 [Accessed 5 February 2019]

Romanosky, S., Hoffman, D., Acquisti, A. (2014) 'Empirical Analysis of Data Breach Litigation' *Journal of Empirical Legal Studies* [Online];11 (1): 74–104 Available from: https://onlinelibrary.wiley.com/doi/abs/10.1111/jels.12035 [Accessed 31 January 2019]

Romanosky, S., Telang, R., Acquisti, A. (2011) 'Do data breach disclosure laws reduce identity theft?' *Journal of Policy Analysis and Management* [Online]; 30 (2), 256–286 Available from: https://onlinelibrary.wiley.com/doi/abs/10.1002/pam.20567 [Accessed 29 December 2018]

Rosenbaum, D. Segarra, M. (2012) 'Unto the Data Breach' *CFO, The Magazine for Senior Financial Executives* [Online]; 28 (8): 20–21 Retrieved from Aalto Finna [Accessed 29 December 2018]

Rouse, M. (2017) *What is data breach?* [Online]; Available from: https://searchsecurity.techtarget.com/definition/data-breach [Accessed 7 February 2019]

Santana, G. (2004) 'Crisis Management and Tourism: Beyond the Rhetoric' *Journal of Travel & Tourism Marketing* [Online]; 15 (4): 299–321 Available from: https://doi.org/10.1300/J073v15n04_05 [Accessed 4 February 2019]

Santana, G. (1999) 'Understanding Crisis and Crisis Management: Towards a Model' In: *Eco-Terrorism: Chemical and Biological Warfare Without Chemical and Biological Weapons, Proceedings of the Chemical and Biological Medical Symposium – CBMTS –Industry I*. Portland, USA: Applied Science and Analysis, Inc. pp. 285-292

Schuetz, J. (1990) 'Corporate advocacy as argumentation' In: R. Trapp & J. Schuetz (eds.), *Perspectives on argumentation.* New York: International Debate Education Association. pp. 272-284

Schultz, F., Utz, S., Göritz, A. (2011) 'Is the medium the message? Perceptions of and reactions to crisis communication via twitter, blogs and traditional media' *Public Relations Review* [Online]; 37 (1): 20–27 Available from: https://linkinghub.elsevier.com/retrieve/pii/S0363811110001281 [Accessed 27 December 2018]

Seeger, M.W. (2006) 'Best Practices in Crisis Communication: An Expert Panel Process' *Journal of Applied Communication Research* [Online]; 34 (3): 232–244 Available from: http://www.tandfonline.com/doi/abs/10.1080/00909880600769944 [Accessed 27 December 2018]

Seeger, M.W., Sellnow, T.L., Ulmer, R.R. (2003) *Communication and Organizational Crisis*. Westport: Greenwood Publishing Group, Inc.

Sellnow, T.L. & Ulmer, R.R. (1998) 'Communication, Organization, and Crisis' *Annals of the International Communication Association* [Online]; 21 (1): 231–276 Available

from: https://www.tandfonline.com/doi/full/10.1080/23808985.1998.11678952 [Accessed 29 January 2019]

Sellnow, T.L., Ulmer, R.R., Snider, M. (1998) 'The compatibility of corrective action in organizational crisis communication' *Communication Quarterly* [Online]; 46 (1): 60–74 Available from: http://www.tandfonline.com/doi/abs/10.1080/01463379809370084 [Accessed 27 December 2018]

Statista (2019) *Number of monthly active Facebook users worldwide as of 4th quarter 2018 (in millions)* (6 Apr) [Online]; Available from: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ [Accessed 6 April 2019]

Sturges, D.L. (1994) 'Communicating through Crisis: A Strategy for Organizational Survival' *Management Communication Quarterly* [Online]; 7 (3): 297–316 Available from: https://doi.org/10.1177/0893318994007003004 [Accessed 2 January 2019]

The Economic Times (2018) *Data leaks damage Facebook's reputation; Tesla becomes most-trusted company* [Online]; Available from: https://economictimes.indiatimes.com/magazines/panache/data-leaks-damage-facebooks-reputation-tesla-becomes-most-trusted-company/articleshow/67320062.cms [Accessed 6 April 2019]

Tierney, K. (2003) 'DISASTER BELIEFS AND INSTITUTIONAL INTERESTS: RECYCLING DISASTER MYTHS IN THE AFTERMATH OF 9–11, In: in Lee Clarke (Volume 11) *Terrorism and Disaster: New Threats, New Ideas (Research in Social Problems and Public Policy.* Emerald Group Publishing Limited, pp. 33 - 51 [Online]; Available from: https://www.emeraldinsight.com/doi/abs/10.1016/S0196-1152%2803%2911004-6 [Accessed 6 February 2019].

Ulmer, R.R., Seeger, M.W., Sellnow, T.L. (2007) 'Post-crisis communication and renewal: Expanding the parameters of post-crisis discourse' *Public Relations Review* [Online]; 33 (2): 130–134 Available from: http://linkinghub.elsevier.com/retrieve/pii/S0363811106001573 [Accessed 2 January 2019]

Utz, S., Schultz, F., Glocka, S. (2013) 'Crisis communication online: How medium, crisis type and emotions affected public reactions in the Fukushima Daiichi nuclear disaster' *Public Relations Review* [Online]; 39 (1): 40–46 Available from: https://linkinghub.elsevier.com/retrieve/pii/S0363811112001816 [Accessed 6 February 2019]

van der Meer, T.G.L.A., Verhoeven, P. (2013) 'Public framing organizational crisis situations: Social media versus news media' *Public Relations Review* [Online]; 39 (3): 229–231 Available from: https://linkinghub.elsevier.com/retrieve/pii/S0363811113000027 [Accessed 27 December 2018]

Veltsos, J.R. (2012) 'An Analysis of Data Breach Notifications as Negative News' *Business Communication Quarterly* [Online]; 75 (2): 192–207 Available from: http://journals.sagepub.com/doi/10.1177/1080569912443081 [Accessed 27 December 2018]

Verizon Communications (2018) *Verizon 2018 Data Breach Investigations Report, Executive Summary* [Online]; Available from: https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf [Accessed 7 February 2019]

Weiner, B. (1st ed.) (2006) *Social Motivation, Justice, and the Moral Emotions : An Attributional Approach.* New York: Psychology Press

Weiner, B., 1985. 'An attributional theory of achievement motivation and emotion' *Psychological Review* [Online]; 92 (4): 548–573 Available from: https://psycnet.apa.org/record/1986-14532-001 [Accessed 2 February 2019]

Weiner, B. (1972) 'Attribution Theory, Achievement Motivation, and the Educational Process' *Review of Educational Research* [Online]; 42(2): 203–215 Available from: http://journals.sagepub.com/doi/10.3102/00346543042002203 [Accessed 20 January 2019]

Wong, R. (2013) *Data Security Breaches and Privacy in Europe*. London: Springer, Retrieved from Aalto Finna [Accessed 27 December 2018]

Yahoo! Finance (2019) *Facebook, Inc. (FB) Stock Price, Quote, History & News* (4 Apr) Available from: https://finance.yahoo.com/quote/FB/ [Accessed 4 April 2019]

Yang, S.-U., Kang, M., & Johnson, P. (2010) 'Effects of Narratives, Openness to Dialogic Communication, and Credibility on Engagement in Crisis Communication Through Organizational Blogs' *Communication Research* [Online]; 37(4): 473–497 Available from: https://doi.org/10.1177/0093650210362682 [Accessed 6 February 2019]

Zainal, Z. (2007) 'Case Study As a Research Method' *Jurnal Kemanusiaan* [Online]; 5 (1): 1-6 Available from: https://jurnalkemanusiaan.utm.my/index.php/kemanusiaan/article/view/165 [Accessed 7 March 2019]

Appendices:

Appendix 1: Table 1 SCCT

Table 1: SCCT crisis types by crisis clusters

Victim cluster: In these crisis types, the organization is also a victim of the crisis.
(Weak attributions of crisis responsibility = Mild reputational threat)

Natural disaster: Acts of nature damage an organization such as an earthquake.
Rumor: False and damaging information about an organization is being circulated.
Workplace violence: Current or former employee attacks current employees onsite.
Product tampering/Malevolence: External agent causes damage to an organization.

Accidental cluster: In these crisis types, the organizational actions leading to the crisis were unintentional.
(Minimal attributions of crisis responsibility = Moderate reputational threat)

Challenges: Stakeholders claim an organization is operating in an inappropriate manner.
Technical-error accidents: A technology or equipment failure causes an industrial accident.
Technical-error product harm: A technology or equipment failure causes a product to be recalled.

Preventable cluster: In these crisis types, the organization knowingly placed people at risk, took inappropriate actions or violated a law/regulation.
(Strong attributions of crisis responsibility = Severe reputational threat)

Human-error accidents: Human error causes an industrial accident.
Human-error product harm: Human error causes a product to be recalled.
Organizational misdeed with no injuries: Stakeholders are deceived without injury.
Organizational misdeed management misconduct: Laws or regulations are violated by management.
Organizational misdeed with injuries: Stakeholders are placed at risk by management and injuries occur.

Table 5 SCCT Crisis Clusters by Coombs (2007)

Appendix 2: Table 2 SCCT

Table 2: SCCT crisis response strategies:

Primary crisis response strategies

Deny crisis response strategies

Attack the accuser: Crisis manager confronts the person or group claiming something is wrong with the organization.

Denial: Crisis manager asserts that there is no crisis.

Scapegoat: Crisis manager blames some person or group outside of the organization for the crisis.

Diminish crisis response strategies

Excuse: Crisis manager minimizes organizational responsibility by denying intent to do harm and/or claiming inability to control the events that triggered the crisis.

Justification: Crisis manager minimizes the perceived damage caused by the crisis.

Rebuild crisis response strategies

Compensation: Crisis manager offers money or other gifts to victims.

Apology: Crisis manager indicates the organization takes full responsibility for the crisis and asks stakeholders for forgiveness.

Secondary crisis response strategies

Bolstering crisis response strategies

Reminder: Tell stakeholders about the past good works of the organization.

Ingratiation: Crisis manager praises stakeholders and/or reminds them of past good works by the organization.

Victimage: Crisis managers remind stakeholders that the organization is a victim of the crisis too.

Table 6 SCCT Crisis Response Strategies by Coombs (2007)

Appendix 3: Table 3 SCCT

Table 3: SCCT crisis response strategy guidelines

1. Informing and adjusting information alone can be enough when crises have minimal attributions of crisis responsibility (victim crises), no history of similar crises and a neutral or positive prior relationship reputation.
2. Victimage can be used as part of the response for workplace violence, product tampering, natural disasters and rumors.
3. Diminish crisis response strategies should be used for crises with minimal attributions of crisis responsibility (victim crises) coupled with a history of similar crises and/or negative prior relationship reputation.
4. Diminish crisis response strategies should be used for crises with low attributions of crisis responsibility (accident crises), which have no history of similar crises, and a neutral or positive prior relationship reputation.
5. Rebuild crisis response strategies should be used for crises with low attributions of crisis responsibility (accident crises), coupled with a history of similar crises and/or negative prior relationship reputation.
6. Rebuild crisis response strategies should be used for crises with strong attributions of crisis responsibility (preventable crises) regardless of crisis history or prior relationship reputation.
7. The deny posture crisis response strategies should be used for rumor and challenge crises, when possible.
8. Maintain consistency in crisis response strategies. Mixing deny crisis response strategies with either the diminish or rebuild strategies will erode the effectiveness of the overall response.

Table 7 SCCT crisis response strategy guidelines

Appendix 4: Data of the bachelor's thesis

Data	Author/	Data source/Headline/Url (Website)	Neg.	Pos.	Date published
Blog post 1 B1	**Rosen, G. & Canahuati, P., 2018**	**Facebook Newsroom** ***Security Update | Additional Technical Details*** **https://newsroom.fb.com/news/2018/09/security-update/**			**Sept 28, 2018**
Twitter post 1 T1	**Facebook, 2018**	**Facebook's Twitter** ***First Twitter post*** **https://twitter.com/facebook/status/1045722820582432768**			**Sept 28, 2018**
Twitter post 2 T2	**Facebook, 2018**	**Facebook's Twitter** **Second Twitter post** **https://twitter.com/facebook/status/1045831261678264320**			**Sept 28, 2018**
FB post 1 F1	**Zuckerberg, M, 2018**	**Facebook, Mark Zuckerberg** ***Facebook post about the breach*** **https://www.facebook.com/zuck/posts/10105274505136221**			**Sept 28, 2018**
Website article 1 A1	Isaac, M. & Frenkel, S., 2018	The New York Times *Facebook Security Breach Exposes Accounts of 50 Million Users Z* https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html	X		Sept 28, 2018
Video 1 **V1**	**CNBC Television, 2018**	**Youtube** ***Zuckerberg says Facebook working with FBI to investigate security breach*** **https://www.youtube.com/watch?v=eMe4tZGVSro**			**Sept 28, 2018**
Website article 2 A2	O'brien, M. & Anderson, M., 2018	TECHXPLORE *Facebook says 50M user accounts affected by security breach* https://techxplore.com/news/2018-09-facebook-50m-user-accounts-affected.html		X	Sept 28, 2018
Website article 3 A3	Perez, S. & Whittaker, Z., 2018	TECHCRUNCH *Everything you need to know about Facebook's data breach affecting 50M users* http://social.techcrunch.com/2018/09/28/everything-you-need-to-know-about-facebooks-data-breach-affecting-50m-users/	X		Sept 28, 2018
Website article 4 A4	Steinmetz, K., 2018	Yahoo! News *Why Should Users Trust Facebook? It's a Hard Question for Mark Zuckerberg to Answer* https://news.yahoo.com/why-users-trust-facebook-apos-193243130.html		X	Sept 28, 2018
Website article 5 A5	Castillo, M., 2018	CNBC *Facebook security breach allowed hackers to control the accounts of up to 50 million users* https://www.cnbc.com/2018/09/28/facebook-says-it-has-discovered-security-issue-affecting-nearly-50-million-accounts-investigation-in-early-stages.html	X		Sept 28, 2018
Website article 6 A6	Wong, J., 2018	The Guardian *Facebook says nearly 50m users compromised in huge security breach* https://www.theguardian.com/technology/2018/sep/28/facebook-50-million-user-accounts-security-berach	X		Sept 29, 2018

Website article 7 A7	Osnos, E., 2018	THE NEW YORKER *How Serious Is the New Facebook Breach?* https://www.newyorker.com/news/daily-comment/how-serious-is-the-new-facebook-breach	X		Sept 29, 2018
Website article 8 A8	O'brien, M. & Anderson, M., 2018	PHYS *What comes next in Facebook's major data breach* https://phys.org/news/2018-09-facebook-major-breach.html		X	Sept 29, 2018
Video 2 V2	TODAY, 2018	Youtube *Facebook Data Breach Affects 50 Million: What You Need to Know | TODAY* https://www.youtube.com/watch?v=ihQhBpgVdyE	X		Oct 1, 2018
Video 3 V3	BreakingOne, 2018	Youtube *The Facebook security breach, explained (September 2018)* https://www.youtube.com/watch?v=qTQXI_ZGC0U		X	Oct 1, 2018
Blog post 2 B2	**Rosen, G., 2018**	**Facebook Newsroom** *Facebook Login Update* **https://newsroom.fb.com/news/2018/10/facebook-login-update/**			**Oct 2, 2018**
Twitter post 3 T3	**Facebook, 2018**	**Facebook's Twitter** ***Third Twitter post*** **https://twitter.com/facebook/status/1047253784248778752**			**Oct 2, 2018**
Website article 9 A9	Fazzini, K., 2018	CNBC *Facebook's muddy response to last week's hack may become the new norm* https://www.cnbc.com/2018/10/02/facebooks-muddy-account-breach-response-could-be-the-new-norm.html	X		Oct 2, 2018
Website article 10 A10	Winchel, B., 2018	PR Daily *Facebook rapidly responds to data breach affecting more than 50M users* https://www.prdaily.com/facebook-rapidly-responds-to-data-breach-affecting-more-than-50m-users/		X	Oct 2, 2018
Website article 11 A11	Guynn, J., 2018	USA TODAY *Largest Facebook hack ever turns up heat on Mark Zuckerberg* https://www.usatoday.com/story/tech/news/2018/10/02/mark-zuckerberg-and-facebook-team-take-heat-massive-data-breach/1490895002/	X		Oct 3, 2018
Website article 12 A12	O'Sullivan, D., 2018	CNN Business *Facebook just had its worst hack ever — and it could get worse* https://www.cnn.com/2018/10/04/tech/facebook-hack-explainer/index.html		X	Oct 4, 2018
Blog post 3 B3	**Rosen, G., 2018**	**Facebook Newsroom** ***An Update on the Security Issue*** **https://newsroom.fb.com/news/2018/10/update-on-security-issue/**			**Oct 12, 2018**
Twitter post 4 T4	**Facebook, 2018**	**Facebook's Twitter** ***Fourth Twitter post***			**Oct 12, 2018**

		https://twitter.com/facebook/status/1050787855965057024			
Website article 13 A13	Rodriguez, S., 2018	CNBC *Facebook says hackers were able to access millions of phone numbers and email addresses* https://www.cnbc.com/2018/10/12/facebook-security-breach-details.html		X	Oct 12, 2018
Website article 14 A14	St. John, A., 2018	Consumer Reports *Facebook Breach Exposed Personal Data of Millions of Users* https://www.consumerreports.org/digital-security/facebook-data-breach-exposed-personal-data-of-millions-of-users/	X		Oct 12, 2018
Website article 15 A15	Tynan, D., 2018	The Guardian *Facebook says 14m accounts had personal data stolen in recent breach* https://www.theguardian.com/technology/2018/oct/12/facebook-data-breach-personal-information-hackers	X		Oct 12, 2018
Website article 16 A16	Maring, J., 2018	Android Central *Facebook October 2018 security breach: Everything you need to know* https://www.androidcentral.com/facebook-october-2018-security-breach	X		Oct 12, 2018